>> ALLAN FRIEDMAN: One can say many things on NTIA, but we work very hard to be prompt and timely.

So with that, Melinda, if you can open the phone lines for the folks who are listening, and those you watching on the webcast, welcome. It is my pleasure to introduce my boss, Evelyn Remaley, to make a few opening remarks.

>> EVELYN REMALEY: Thank you, Allan. It's good to see everyone. That was actually a very provocative opening. So hopefully no one is saying bad things about NTIA, but if you are, you can let me know afterwards. But good to see all of you. I just want to thank everyone for coming in for this, and to those of you who are taking time out of your busy day to watch this and join over the phone. I know that we have some folks planning on staying up late across the Atlantic and some already awake across the Pacific for this. So we're so pleased that this has truly become a global initiative, and all of you are to thank for that, so we appreciate it.

Second, a thank you to Allan for his tireless commitment on this effort. He's like the chief internet security wrangler. I don't think he really saw his role as that while he was pursuing his PhD, but we're so happy to have him with us to do this good work, and that's really invaluable.

This is our sixth meeting, and we've heard from a number of folks both in industry and government how impressed they are with the progress that you've been making. This has gone from a controversial idea to a well, not-so-quite-controversial one, at least in some circles, and an obvious idea to others. We've picked up friends and allies along the way and learned that many of us across the entire community understand the real need to know what is in our software supply chain.

From my own experience, I can tell you that I know -- I now hear my senior government counterparts who are interested in software-defined networking for 5G or securing the ecosystem for IOT referring to SBOM, which is pretty unprecedented, let me tell you, and a real win in my book. So again, that is all really an acknowledgement of the great work that you're doing in this group.

Looking at these drafts, we'll be talking about today, it's important to note just how far we've come since last fall. You've been at this for just over a year. That's pretty fast progress for a consensus-building process and especially fast for an initiative that spans this many perspectives, interests and needs. We know that today isn't the end. We've heard from you that it's not just enough to publish a few white papers. We have to keep working on this, though great documents they are, and I was very impressed walking past the drafts outside today. So thank you.

After we've had a chance to give these drafts further review and discuss the further progress made, we'll pivot to talking about what's next. You have told us that you'd like NTIA to continue to host this discussion and help facilitate the work you have left to do. So this afternoon we'll be going over what that can look like. In addition to giving all of us some next steps and more work, it's also a chance to take a step back.

What is our vision going forward? What should S1 look like as we move from crawl to walk and then run? What tools do we need to make this happen? How can we promote awareness and adoption outside the NTIA community and around the world? Who are some of the new partners and voices we should be bringing to the table?

Lastly, I want to take the occasion to remind you that this is your process. NTIA is just here to facilitate. We are completely committed to that and to helping you work through these genuinely challenging issues. If this was easy, it would have been done already. We know that.

Good luck today. We're confident that with this group of experts real progress making the software supply chain more secure is possible.

And again, just thank you very much for your commitment. We know that you all have day jobs, but we are just hearing so much good response in terms of the work that is being done. So we appreciate this moving forward.

And with that, thank you, and I'll turn it back over to Allan.

[APPLAUSE]

>> FRIEDMAN: Thank you. So we have a full day. As Evelyn mentioned, we have some pretty spectacular graphs. We know that they're not complete just yet. They need a little more polish. And, of course, this is a chance to give real feedback, finally. We've seen them evolve. There's a chance to get final feedback before we find consensus on them. What we want to make sure to do is this morning we're going to cover these documents, and for those who've been participating before or watched this before, we'll hear from each of the four working groups to sort of say, "Hey, what's changed? What have they been working on? And if anything -- if they want attention to any last details and feedback on any last details.

We'll take our lunch break, East Coast time, 12:15-1:15. And then we're going have a chance to pivot, not just to capture and try to say, "Were there any other issues that we want to tackle that were raised in the morning?" Let's sort of identify what are some of the next steps. And that's a chance to be a little creative. We'll talk a bit more about that after lunch.

So I guess it's a little late to offer the reminder to silence your cell phones. But what we can do is encourage you. This is a chance to chime in, to engage. For those of you who are new to the process, we're really happy that you're here. There's still a lot of work to be done, and it's going to be much better if all us roll up our sleeves and pitch in.

>> ALLAN FRIEDMAN: So thank you. It is my pleasure to start by inviting Art Manion, who is one of the co-chairs of the framing working group to talk about what is an SBOM, and how they've tried to sort of document that. Art does have slides. Ok. We'll put them on that sheet. Sure.

>> ART MANION: No worries. Thanks, Allan and Evelyn and NTIA. My co-chair, Michelle Jump, can't make it today. She sends her apologies, but we've talked a bunch in the last three or four weeks. I think I've got everything pretty well synchronized between the two of us and the Framing Working Group.

What I'm basically going to talk about is just to highlight the changes in the document since the last in-person meeting. It was, only a other than general cleanup, which there was plenty to do and still more to do, there's four or five kind of major things that if you are looking at the difs, basically you'd want to pay attention to. So those are sort of as an overview -- the beginning and end of the document have changed. A conclusion which is a brand new section was added. We moved some of the intro material from the intro to the end, reorganized the intro material. So first and last parts of the document got some changes. We added an acknowledgement section, not a major issue, but it's time to start thinking and noticing those who have been in our working group and contributing to this whole document.

One sort of conceptual thing that's been going on throughout the whole year more has been what I'm going to call sort of, "Which way is up or down in the tree orientation?" [INDISCERNIBLE] and I had a discussion the Week of the Black Hat and Def Con and Be Size conferences about which way we visualized the supply chain sort of graph or tree. And it turned out for the last year, we had opposite ideas, that was probably causing a little bit of communication error.

So we sort of worked that out and then as I was going through this document last week -- I think I'm flipping it back again. If I get the slides, which is entirely my fault for being too late, I'll show you the picture I've got. But this is represented in the document. We have a table representation of how an SBOM might look, and we have a tree or a graph. I mean, graph database, not just whatever kind of graph, not a graph, like a numbers-plotted the graph. Does that come -- Okay. Yeah. Yeah.

So if I say the word "upstream" in a supply chain, that's a part I'm getting from my supplier, and it's got the word "up" in it, and I see no other way conceptually that that can't be sort of north on the piece of paper. I think anything else is going to cause a massive confusion. I think practices is right to left, which is fine --left to right, sorry. Left the right. So smaller parts in the left flowing towards the final assembled goods on the right. Framing's group is take that picture and 90 degrees to the right. I was very concerned that if we had it completely inverted that up and down or backwards, we'd have further no end of confusion.

So if you imagine a tree, the kind of tree that grows in the woods, right. Rip it out of the ground and shake all the dirt off, you have the roots exposed and the leaves are on top. Turn it upside down. Right. Your root suppliers are on top. Your upstream suppliers. All these dependencies and chains happen. And at the very bottom somewhere are end-user organizations that produce nothing, and they are leaf nodes in the tree.

Does that verbal explanation make sense to folks? Does anyone want to disagree, because now would be a good time to do so?

OK. Other than the practice's group having it horizontal, does this conflict with anyone else's work or break anyone else's sort of conceptual paradigm or break the papers were working on?

You're okay with that? Yeah. All right. Also, in terms of the examples, we did sort of collectively come up with across, I guess, three of the working groups the same standardized toy example, so that's resolved, I think, at this point. I don't know if practices is on board with that. It may not matter to your document. Standards and formats and framing or using the same examples, so that we don't cause more confusion.

Furthermore, from the framing group's point of view, we had a number of sort of sample SBOM examples in our document. Those are all gone except for the table and the upside down tree representation. We're going to point to standard formats., who did the actual work on reviewing the existing formats and point to their examples.

So things like Suede and PDX, obviously, package URL. A couple others are in there. So the acknowledgement that things exist and you could represent SBOM in them is handled elsewhere.

Sorry, I'm just going through my notes here.

That's mainly it for the changes in our doc since then. I don't have a whole lot more to add. Most of the work has been -- there's been some actual editorial cleaning up language and punctuation and things like that and formatting. There's been some more material work. I think we're basically dealing with a lot of duplication of document and making sure we have two sections that say the same thing. We only need one of them or two sections that cover the same topic and don't quite agree. We have to work those things out. I think we're down to one of those class of problem left and our clean-up at that point.

Thank you for your noble efforts, Allan. Yeah. This is the important part here. That's the graph version. And you can see this superimposed upside down tree. That's what I was drawing with my hands in the air a minute ago.

So I'll leave this up for just a moment. And just going to for last for the last time, hopefully, if this is OK with everyone.

You obviously can ignore us and not do it this way, but this with the framing group is going to say is the way to think about it. So sorry about that.

>> DUNCAN SPARROW: Thank you. Duncan Sparrow. So I guess two-part question. One - is that upside down tree is not in the document, right? That's just for you explaining it to us?

>> MANION: The actual tree image is not in document. This is in the document. Yeah. Actually that is probably in the document. There's an even smaller version of that that's simpler. It's just the right half of that area.

>> SPARROW: So my actual question, which might get punted to this afternoon when we get into real issues or whatever, but is: Is what the graph -- when you showed a tree, that's clearly a tree. So it's the whole thing. When you're showing this one -- stay in that spot for a second. Is it clear from this document whether that is one SBOM or eight SBOMs? The all infamous one-level n-level, is it addressed. or is it still punted?

>> MANION: Off the top of my head, I would say it could probably be made more clear. The answer is, not to be glib, the answer is yes. It is all of those things. You can focus in and say -- you can make the

SBOM be what you consider it to be. It can be one small branch, one small node. It can be the entire, literally, the global single one, if you had a big enough amount of memory or storage or something. In the paper, we have just the right half of this. That's an SBOM. When I put this together, I could say I have two, or that could be one. It a little bit philosophical, but the nature of the relationships and the dependencies, I think is such that we have to allow this sort of, not quite arbitrary, but you can select the scope that works for what you need to do.

In this example, if I'm that end consumer, I want all of that, right, to know what I have, right. If I'm Acme Software, I only care about my branches from that point, back up, right, but to some extent. Again, good point. I think probably we can be more clear about the infinite recursive nature of the thing. Right?

>> JOSH: I'm absorbing the upside down tree and, pardon the pun, it does seem unnatural to have a tree upside down. My vague suggestion is that we talk across the four teams and pick an orientation. I know you're offering this up as the proposed one, and I can explain when we have more time why I think you probably don't want it the other way. It's because I think the root building blocks don't change very often, but the products built on top of products built into our products will continue to bloom and flourish.

But to his point, my real reason for raising my finger, there's still some confusion among some of the MDMs. Like, for example, if you're an Acme medical device maker and you're using one of my products for my day job, which many of them are, they want to list my product and stop there. And for this to actually support the vulnerability management use case that started a lot of this, am I affected? Where am I affected? People would need to know what's in my supply as well. So whether it's one hops or two hops even wrapped around the axle, I'm hoping as we come near the end of Phase 1, we can at least make it painfully obvious with a visual of Josh's node. And beneath has the vulnerable component, and if you don't look past Josh's node, you won't know you have the vulnerable component. So what we call it, the nomenclature we use is less important to me, but a side-by-side example of one that's too blind to help and one that's comprehensive enough to be useful would be an exit criteria for me.

>> MANION: OK. I believe that is basic to draw those two pictures. I think that's doable, and I'm happy to talk more about orientation, but again, the thing that really flipped me back around was if I just say the word "upstream," I just can't -- we can talk about it later.

That did bring up another point, though, quickly. In this picture, you'll see these boxes with the dash lines. We've wrestled at least on the framing, and I think the standard and formats actually group as well with -- and Josh brought this up as well. Right? If somebody just wants the list of things I'm doing, I include that. That's one thing. If they don't want further, that could be a problem. What if you don't know what's further? And can you convey the knowledge there's something else? There is lack of knowledge, there's something else? There's no assertion, there's something else? I am telling you I have all of the something else. That's a hard question to nail down. The standards and formats group came up with an option. We have it in the framing document currently. I don't know if the standards and formats group still likes that option. So that's in these dashed lines here. It's in the document at the moment. It might be subject to revision or even removal. This is translucency, so I don't know where we ended up on that. Yeah.

>> FRIEDMAN: Sorry. Just as a process question for those of you who are listening in on the phone. If you have a question, hit star one and you'll get on the question queue. Right now, I'm not showing anyone, Melinda, thanks.

More? Are there further views about orientation? And, again, for simplicity -- I have many mics. Right? So again, looking just at this part. This is the chance to have this conversation as we do it again.

>> DOUG: Well, I would say we should punt it to this afternoon. And I think questions of substance like 1-level or n-level take precedence over questions of how nice it looks. If you did want my opinion on how nice it looks, I do think Sideways gets around the upstream downstream problem, because rivers can come from either the right or the left, but upstream, everyone always wants up on top. So I do think that picture's upside down, but actually don't care. I'd rather care about substantive issues.

>> JOSH: This may not be actionable, but maybe one way to clarify this, irrespective of the orientation we choose, is making it clear what those parts versus compound parts versus final goods -- if there's some sort of denote -- If we could denote because final the dissembles are the ones that go through procurement. Right? The ones that might get regulated in operator environment. So maybe just even swim lanes or a backdrop to this. The orientation won't matter if people can cleanly tell this is a small thing being aggregated into a bigger thing.

>> MANION: And I fully agree. The orientation doesn't -- as long as your consistent, it doesn't matter what direction is. The graph math works out fine. I don't really care in that sense. It literally came down to us reading Wikipedia and it said words "upstream" and "downstream" and I thought anything other than this would be horribly confusing. So that's all. That's where I went. That's it. So, yeah.

So I wanted to pick up on Duncan's point around depth. And I think it's important to clarify the work that Art has done in setting the bare minimum versus what someone else may ask for, be it a downstream partner or a customer or a regulator. And I think we will have someone from the FDA this afternoon who can clarify the FDA's position. I know a lot of you are in the medical device community where that's very relevant. Anyone else want to touch on the depth question?

>> FRIEDMAN: I hate being a repeat talker here. One thing I said to some folks this morning is as a key supplier to a bunch of medical device makers in the pilot, none of them asked me for my SBOM. And my expectation fully was, "You're not to be able to provide a comprehensive multi-node SBOM unless I give you mine. So it doesn't mean that Phase 1 was meant to be comprehensive. It just means that if that bug happens to be in mine, and you don't know what's in mine, then your operator hospital won't know what's in it.

>> MANION: Just so that -- I'm going to say that the framing group's position on this is the thing we are -- the model we're building or designing or proposing fully supports as many hops as you want to go. The recursive change in this dependency-ness is built into the model's design. The argument about how many hops you want to go -- we're sort of agnostic. I think it should be everyone does their job. The whole thing falls together. But the framing group's not going to solely argue that it's 1 or n. The model supports all of these things, or the model won't work is our starting position. Sorry, Duncan. Yep.

>> SPARROW: Thank you, Duncan Sparrow. So the use case group maybe wasn't as recognizing the issue of that that would stay open. I think it's actually use case-dependent, what you need. So I think probably we have to take it upon ourselves, so I'm putting Josh to have to change his stuff on the fly here, before he talks, but we probably have to point out that the vulnerability use case assumes the - it's an n-level deep, that if you only have one level, then, yes, you can do a certain amount of vulnerability, but you missed the ones in the end. You shouldn't assume it.

So using his specific example, he sort of blamed the device manufacturers because they didn't give the SBOM. But in the particular model they were following of one level deep, it's up to the consumer to do that. So it's really the hospitals that didn't do it. So all you hospitals that didn't do it, you might want to be the ones yelling at your vendor as opposed us. Thank you.

>> MANION: And this happened. I mean we talked about the vulnerability management use case for a moment, a couple times here, but licensing is the same thing. If I don't see the component three hops deep that has a GPL on it, I mean -- so again, from framing group, we're being a little bit application agnostic. The model has to support this, or model won't work. And then you want to come and put your application, go nuts. We were trying to build something that will support your application without telling you what your application is. Someone else who is an expert in that field can come along and do that. And if our model doesn't work, then we have to adjust from there. So, yeah.

>> FRIEDMAN: Art, I think a lot of the approaches of one from your group was built on two assumptions, one in a tradeoff between maximum utility and ease of adoption.

At this stage we want to prioritize adoption and to if we can actually get that adoption story working, then recursion will give us the depth. And this is a chance for folks to say that is absolutely ludicrous. But that, I think was the thinking that went in the sky. It was discussed a lot.

>> MANION: And again, the model design supports recursion. If you choose to go one layer and have a single flat list or a spreadsheet model allows that, that's your choice. We do provide for the --

>> JOSH: I think scientifically that's fair. I think practically to his point, if we were to map specific use cases to minimum depth, what you'd find is a one hop only will support, I think, nearly zero use cases.

>> MALE SPEAKER: Yeah. I fully agree. Yes.

>> LORI CORSPIN: I think there is also an issue of that if you're taking this into the vulnerability management, the use case, then it will become like how far I have to go, it will then be depending how much those components are overused or reused in the other places, that will be resulting in your impact calculation. And at some point I envision you cannot really have really full picture at all, all the time anyway. I don't think that's really realistic. But when you are putting together your software, your operation or deployment, then you have to be able to manage the forthcoming risk. So you have to be able to see so far as it's important for you. And in this sense, I think it should be also included that when this becomes active, when the particular vulnerability or something will happen, then you are able to go back and start enumerating the other places where it's also having impact. And that's a very important component in the operation later on, not so much that you have the full picture from the start.

>> FRIEDMAN: Thank you. Lori, can you -- I think many folks may not know you. Can you introduce yourself to the crowd? Can you introduce yourself?

>> CORSPIN: Oh, I'm sorry. My name is Lori Corspin [phonetic]. I'm working with Ennis [phonetic] Corporation, and I'm coming from Japan. So I'm kind of in between the U.S. and in Japan. Thank you.

>> FRIEDMAN: Any other comments or questions on this depth question?

>> JOSH: And building on your point, at a current state, it would be quite difficult to get a comprehensive map. Our belief is as these tool chains spit them out as a byproduct of doing their packaging or builds, getting a more comprehensive thing will be a byproduct of how we compile software. So current state, harder to get comprehensive; future state, much more comprehensive.

>> MANION: The vision is to actually have a pretty comprehensive list ahead of time so that when something does come out, you find all those vulnerable nodes quickly and can act accordingly. But it's hard.

>> FRIEDMAN: Further comments on this document or what Art has had a chance to say?

>> LES ABBOTT: I've got one. This is Les Abbott. So I don't disagree with everything that's being said, because I think it's being said in different forms. One thing I would disagree with is that I think one hot or 1-level isn't a zero, though, right? Yeah. So I'll just make that clear because I think --

>> MALE SPEAKER: It's one; It's not zero.

[CROSS-TALK].

>> FRIEDMAN: The entire process agreed that 1 is not 0. Consensus achieved. Good. Yeah. Done. 1 is not 0. Publish it.

Anything else that folks want to add in this?

So, Art, we can provide further details, but if folks who have a chance to read this document and want to provide further details, is there -- I'll communicate after this? Do you have a timeline or some mechanism what you'd like right now?

>> MANION: Sure. So you know that the sort of the dif stuff highlighted in this depth and orientation of the graph, the areas I've highlighted, if you have specific concerns about those, the sooner the better. You're welcome to contact me. You're welcome to put a comment in the Google Doc. Get in touch with the entire framing working group. Get on our mailing list if you'd like. Those things are important. If we don't resolve them, that's postponing the delivery and finalization of the document, basically. Otherwise, if you read the doc, and have anything else to say, I think at this point, our preferred mechanism for feedback is still just a Google Docs. Anyone with the URL can type in changes. They become comments. It's the normal Google Docs trick. We're doing all the work in there. So that's our wish. And please, at this point in the process, also, if you've got a thought or an opinion or some words to change, just go do it. Comments saying, "This could be cleaner," -- we're not going to probably -- I will try to get to them, but basically, provide what you think should be there, or your comment is less likely to be actioned just for time purposes.

>> FRIEDMAN: For clarity, you'd like that in suggestion mode, not edit mode.

>> MANION: Yeah. So it is configured properly. Two or three of us have edit mode; the rest of the world, if you have the URL, you are in suggestion mode, assuming ACLs are right, which they are. That's how it works. But please feel free to just type in there. That's the easiest thing for us. So, yeah.

>> MALE SPEAKER: And you didn't mention a timeframe on that. Are you just going to stay forever. Or are we actually hoping to get it out at some point?

>> MANION: Whatever. Four weeks? I think it's a discussion for today, but we want to be at September, end of September.

>> KATE: Why don't you go for the middle of September, so have the recovery time?

>> MANION: Sure.

>> KATE: So September 15th, maybe?

>> MANION: Yeah. Give me a couple of Fridays into September. Right.

>> FRIEDMAN: That's ten days. You want to do two weeks?

>> KATE: Two weeks? Yeah.

>> MANION: Sure.

>> FRIEDMAN: A two week window? We'll revisit the overall process a little bit later. But I think that is a good benchmark to start.

>> MANION: Yeah, two weeks is enough time for us to finish the doc, even if we get no comments. but if you do have things to say, yeah. And again, if it's about the fundamental parts, please, please, please very soon, because we need time to resolve those before we go finish the writing.

>> FRIEDMAN: And for folks in the room or watching, if you would like a copy of that URL, I will try to send it out with the notes from today. But you can also reach out to me directly, and I can send you the up-to date-version for that URL.

Any other questions for Art or the framing group?

Melinda, I'm not showing anyone in the Q&A queue.

>> MELINDA: Thank you. No phone questions at this time.

>> FRIEDMAN: Great. Thank you. Duncan.

>> SPARROW: One more. Sorry for hogging the mic. Again, because Art is up first, he gets stuck with all of these, I'll call them process questions. Is it appropriate to ask now next steps, or is that a leader agenda topic? Are we going to do it by committee or do it by all at once?

>> FRIEDMAN: Both of those are phenomenal questions, and we're going to try to tackle that after lunch today. The goal of this meeting is to sort of say, "Let's focus on this Phase 1 for the moment," and then were going to say, "What will the next phase look like?".

All right. Well, thank you, Art, and for those -- hope you can get a copy outside of this document, and there's still a little bit of work to do, but you guys have done a phenomenal job. So thank you, everyone, who's been part of that process. I know the weekly Friday afternoon calls are a bit rough. And so thank you all for doing that.

>> MANION: All right. Thank you.

>> ALLAN FRIEDMAN: And now we have Josh Corman from Use Case Group. So those of you who know me know that I do a decent amount of talking about SBOM or perhaps never shut up about it, depending on your perspective. And we sort of think about framing group as the what is the SBOM, and the use cases group has really done a great job of drilling down into the why is a use bomb -- why in an SBOM?

>> JOSH: I sent my slides ahead of time.

>>FRIEDMAN: You did! The surface is [INDISCERNIBLE]

>> JOSH: So when we last saw our heroes here in the use case group, we had a pretty well fleshed-out document, and we were soliciting input on some other parts. We had two sections we had yet to write. I'm going to spend the bulk of the time I have on the two newer sections, but I'm briefly orient people to what we had done before, in case you're newer to the process.

>> JOSH: In this document we set up -- beautiful. So how do I click?

>>FRIEDMAN: This space?

>> JOSH: So we've had varying co-chairs on this over time, lots of participants and too many to think specifically. Some of you -- back to the vertical versus horizontal orientation, we've kind of taken a left to right idea that there's -- in the nomenclature, we've tried to use in the document, so it becomes useful, is that there are individual parts like an atomic written open source project that does a single thing. Compound parts. This could be things like a really big open source project like Apache struts, or it could be a commercial thing like a real time operating system, or it could be industrial i-platform like I build in my job.

Then they ultimately get assembled into a final goods assemble, which is purchasable, sometimes regulated. In this case, we've used the metaphor of a bedside infusion pump made by a medical device maker, and then those get purchased by various operators or hospitals. Within every leg of this chain, the supply chain, you're -- most of us are in the middle. There's upstream and downstream, but most of us are in the middle. And in a more detailed version and some previous things you won't rehash, there were really three major categories per stakeholder, looking for, if you're a Demming fan, it was choosing the best suppliers to depend upon, choosing the best supply from those suppliers during your go live testing or whatever. And then operational vigilance for the lifetime of that dependence to see new vulnerabilities or glitches or things to fix.

What we've done in our paper in lido is we've argued this at more consumable on-roll, and essentially those roles will be listed here. If you just drill into operator, even all three of these roles exist at all legs of the chain, we left Demming behind and we said, "There are people that produce software; there are people who choose software; and there are people who operate software," and the orientation of the document -- I'm stealing this beautiful slide from a government employee. But these are some of those things that we went really deep on. In this way in the orientation document, if you're reading this document and you're in this role, this is, "What's in it for me?" the WIFM. This is, "How can I benefit as a single part of a complex supply chain by having an SBOM or tracking SBOM? What are the tangible benefits to my business?" And they're not all security. In fact, most of the adoption you saw in the financial services world was massively increasing developer productivity by having less unplanned, unscheduled work, fewer break fixes, faster mean time to recover. So it became an operational boost, which is why I got a lot of legs, independent and irrespective of security. So those roles help someone who cares about , "Why should I care about getting interested in the SBOM stuff?" and it's very tailored.

What we've done, though, and this is from last time. So what we've done those we did have a placeholder that says the real benefits happen with network effect, and when we have compounding security debt with interest, what's the compounding benefit if we get it right? So we start introducing the concept and now we have it in prose form of, "Could you accelerate the entire thing?" Now, if you're from the medical world, there's this notion of patient health, which is the relationship between you and your doctor. How do we treat your ailments? But there's also public health, which , "What's systems hospitals' herd immunity, vaccinations, access to care, efficiency of care?".

So these are really taking a zoom out to say, "Could every single one of us that has a very localized benefit understand the systemwide benefit if you project into the future?" And I want to applaud everybody in this project. It's hard to project into the future. If we had X, what would that look like? It's like taking apart a Lego diagram and projecting into the future and seeing what happens next. It's not an easy thing to do. I think in hindsight, this group will look back and say, "Why did we not do this always?" This is such an obvious idea in hindsight, but projecting the future is difficult and I applaud the group that's done this.

So again, we believe those systemwide public health benefits become dramatically accelerated vulnerability management in the footrace between adversaries and defenders. And we'll show a graphic in a moment.

Number two. It's not just herd immunity, as we start to choose better suppliers, but amplified herd immunity, because it's not a one-to-one thing, like you would see with vaccinations; it's one too many.

Number three is we've debated over the name of this, but we believe a natural byproduct of this transparency will be that poorly maintained projects with incomplete SBOMs or no SBOMs who never fix their bugs will die off or we will migrate away from their use, which also further amplifies the prior herd immunity concept. So notions that some --we will migrate towards higher quality suppliers.

And then lastly, because it's just a feature of the system that some suppliers go out of business or get orphaned as open source projects, and currently that's a very disruptive event in the presence of a world with SBOMs, it's a non-event. So quickly showing those graphics.

Thanks again to our resident artist who spans a couple of these. We took those motifs of a parts supplier, a compound part supplier of final goods assembled, and an operator with those shades of purple, and essentially, some of you have heard me say this before, but upon the revelation of a new vulnerability, there's a foot race between adversaries and vendors. The adversary is, I call it, mean time exploitation. So the mean time exploitation now is being measured in days or weeks. That's the unit of time. The mean time, to remediate for the multi-legged relay race here is measured in months and years.

So we took an interview of one of our stakeholders who had a vulnerability in an open source project. It took six months. So basically that open source project had a vulnerability, if we're looking at the top bracket. When they learned of it, six months to digest, fix it, test it and safely and quietly communicate it to their customers.

So that starts the next leg of the relay race. That little exclamation point is the first moment in notification for those medical device makers. They do some initial triage. They take it in. They test it. They fix it. They put it through its quality process. They check in with the regulator. They push it to the hospitals. So it's a multi-legged relay race that spans actually years, and we took the numbers from that actual disclosure.

Imagine a world of SBOM, though, with this little yellow piece, which is the ability to mitigate while you're waiting for later remediation. If there's contemporaneous impact assessment of, "Oh, that hospital knows on day one that they are affected by this particularly bad thing, they may not be able to put out a patch. The patch is still being developed, but they can take mitigating controls or steps to either segment the network, shield it, take it off line, find some other alternative to increased visibility.

But the idea of that footrace being compressed, it does not compress the work of later remediation, but it absolutely compresses the window within which people can know and respond. So mean time to identification, mean time to mitigation, while we pursue and wait for the longer term remediation,. Son this graphic can be stared at. Basically the top bracket is without SBOM second ones with SBOM. And part of the idea here is to give a heads up to every downstream dependent irrespective of what their manufacturers tell them.

>> JIM JACOBSON: Josh - can I ask a question? On that slide or that graph, it really depends upon the -- that the communication today is quiet communication, right. It's information that's provided often just to the consumers under certain circumstances.

>> JOSH: Yeah. I would say we had more complicated ones. Maybe we should share them with folks later, but some of them are triggered by a public exploitation, in which case the whole world knows. But their hair's on fire. Some of them are quiet, coordinated disclosures through NDAs or customer relationships.

>> JACOBSON: But in that case, you don't get -- everyone is starting at the same time.

>> JOSH: That's the top. So we took an actual story, start to finish, and the hospitals that were affected didn't know for quite some time.

>> JACOBSON: Right. But in order to do that, it requires a change in how vulnerabilities are communicated and in addition to SBOMs.

>> JOSH: I'll take one more attempt for now to see if I am hearing you correctly. In lieu of an SBOM, they were dependent on their notification from their vendor discreetly. In a world where they have SBOMs, they would know that, "Oh, there's a new flaw in log for J, version X dot Y dot Z. I have log for J, X dot Y dot Z Let me take precautions so I don't get hit by the attack in a while.

>> JACOBSON: But exploitation is advanced as well.

>> JOSH: Yeah, potentially.

>>FRIEDMAN: And if I heard Jim's point, the hospital would need a mechanism to know about the vulnerability of log for J.

>> JOSH: Yeah. In fact, what some of the hospitals currently do is they'll take the SBOMs they've been given from their partial list of suppliers that provide them, and they have scripts that just watch the national vulnerability database and give them a local alert -- that type of automation. That's one of the key reasons we pushed so hard in day one. These should be machine readable and ideally in consistent formats because that facilitates more machine speed, vigilance versus human vigilance.

I have a few more slides to get through, and we can come back to any of these if you like. Number two is the idea of herd immunity. So most people know that if they vaccinate a certain percentage of population before it takes root, when you reach a critical mass, like you have a population immunity versus individual immunity, it's harder for diseases to take root.

We have kind of a public health issue. One of the unrelated to this project, after the [INDISCERNIBLE] Act, but not there was a lot of domestic and international, even state and local level people saying, unpatchable devices with hardcoded passwords are a public health issue. So the herd immunity concept is if we vaccinate enough of them, or if there are enough of them that are immune to these attacks, the attacks don't spread as fast.

This is compounded if -- I'm dating myself here. But if you remember the Fabergé commercials of, "I told two friends, and they told two friends, and they told two friends," because these are one-end relationships at each hop, we get an amplification of herd immunity as we invest, or the inverse of that is current state is we amplify harm. But the amplification effect plus network effect was when the concepts we have a bunch of prose on speeding up a little bit is we also believe a natural consequence. We've already seen this in the financial services folks. They start making lists called -- one of the banks, uses a list called a prohibited technology list. So as they get the SBOM, they scan for certain projects that are really risky or have burn them in the past.

So as people start to scrutinize either abandoned projects, projects that can't provide an SBOMs, other things, I think certain projects will have less dependence will migrate and shift some. I was talking to a major software supplier in the back who's already kind of doing that.

A natural byproduct of transparency is we gravitate towards better goods. So we believe that this means some of those high-risk projects just won't get much patronage. So they'll be fewer and better projects, which is very Demming sounding.

And then the last of these discrete ones we talked about is it's currently quite hard -- the House Energy and Commerce convened a stakeholder meeting around the cons of SBOM a couple of years ago with bunch medical device makers and hospitals. And one of the hospitals said, "I don't need an SBOM. I can just -- my vendor can tell me if they're vulnerable." And we pointed out how many devices they have where there isn't a vendor. The vendor's out of business.

So one of the things that a manual business relationship depends upon is that your entire chain is still active, vibrant, and hasn't been acquired and reacquired an end of lifed and what not. So in a world where we're baking in an SBOM at the time of creation, those SBOMs can live on much longer than the organization behind it. So this is more like future-proofing. Sometimes we call it extinction-proof for out-of-business proof, but that red spot becomes a blind spot for everything prior. But if we're concurrently providing that SBOM of the version delivered at the time of the creation or delivery, you have some resilience in the system.

And then again dating myself, but the comminatory effect of, you know, forming Voltron from all these is started to get really exciting.

You get a very short paragraph or two in there, which is if you can imagine any one of these benefits to the system, but putting them together, if we truly weed out the bad derelict projects and we amplify those higher quality, better maintained projects through network effect and amplification, and we can have prompt and agile notification at any leg of that relay race in the entire dependency tree, sideways, up, down, left, right, it starts to unlock some pretty cool things where we're not going to have 50 different versions of a competing library. We're going to have a couple really solid, well-maintained ones.

If someone won't provide an SBOM because they're a free open source project with volunteers, people probably won't use it much anymore. Or if you have one that has a mean time, one of the ways the banks track this or you guys know Jim Ralph, who's been pioneering the space, they would track the metrics of when there's a new vulnerability in these projects, what's the mean time to remediate for the project and some meet MTTRs 30 days. Some of them, over a year. So as you start to track performance over time, because now you're able to measure them, it becomes much easier to know good from bad vendors or good from bad open source projects.

So there's a whole bunch of comminatory effects and cumulative effects. We start to explore that section. It probably got the least review, but I would love people to poke at each of those four discrete ones or look at the comminatory. We left a few on the cutting room floor as well, because we didn't want this to be a super-long document, but again, it was accelerated vulnerability management across the whole relay race. It was the network effects for immunization or herd immunity multiplied by the 1 to n relationship. It was, we believe, inevitable secondary and tertiary effects of supplier selection or survival of the fittest supply. And then lastly, the ability to weather or persist on your use cases irrespective of the longevity of the supplier up and downstream in the chain.

So I think that's what we have for section --there's one more thing which I think Bob Martins here -- and will speak for himself when we open it comments. But the other section we added is an appendix was some of those higher assurance DoD things. And these would be things like provenance, pedigree, integrity. What's the chain of custody of this thing. And not just that this is the version number and some hash. But do we know who compiled it? Do we know who touched it along the way? Do we know where it was hosted? So some of us maybe Phase 2 or specialized use cases for national security level or military use cases. I believe they'll end up becoming pervasive use cases eventually in the free voluntary system. But there's some acute pressure to get this stuff tackled earlier, and we have a whole section on that now in the appendix.

So the two newest sections in summary are we had the public health view versus the microscopic view of people who produce software, choose software, operate software. And also, we tied it back to those selfish interests because any of the benefits you thought you might get as one of those three stakeholders only become better as the network effects kick in. So the act of SBOMing will provide immediate value, but the longer term value of lots of people SBOMing provides significantly more value.

To sound like a little kid, I got kind of giddy when we were writing that last section of the comminatory effects because it truly gets exciting when you project into the future that these are more commonly available byproducts of build and packaging tools and we gravitate towards things that can actually support these intents, the world looks a lot less vulnerable. I know that vulnerable management is but one of our use cases. I think it's a pretty critically important one, since like I said, mean time exploitation is days and weeks. Mean time remediation tends to be months and years. We've got to change the math. This is one way to change the math.

>> FRIEDMAN: All right. Thank you, Josh. There's one other part of the document that I want to flag for folks, which is a set of related projects that highlights the potential for transparency, that this is something that we're seeing in all different corners of the community, whether it's the business software alliances framework or some older documents from various different sectors. So this is something that is useful to sort of see, "Oh, look. This is coming from a lot of different areas. This isn't just the people in the room who had this idea has been around for a while."

>> JOSH: Oh, and I guess just to punctuate what Duncan said back on this graphic, so if on that white pipe, the compound IOT platform that's in a lot of medical devices, and that's my day job, by the way, if we stop at -- we use that white pipe, then you may not know that the hospital is vulnerable. If you go back a step and say, "Oh, there's a new vulnerability in some version of Apache common collections I'm using," then you'd say, "Oh, crap. I have something I have to do."

So that's why we believe to support the minimum viable use cases for things like vulnerability vigilance for that, the operating environment, it does require multi-hop, which your framing group is agnostic to. I fully appreciate that. When the rubber meets the road to actually get people we want to have -- 1 is more than 0. Multi-node, especially if it's readily available, is significantly more valuable. Very few comments.

>> FRIEDMAN: A couple here.

>> LORI COSPIN: Ok, so I have a question. You are working right now on focusing on the survival of the fittest, but are you also focusing on how to improve the existing ones so you use it as an education tool first of all?

>> JOSH: Yeah, I mean, we wrestle over even how to describe that section, but there's an opportunity for four projects that weren't doing good hygiene to say, "Wow, we could we could do a lot better. Let's do that." There's other projects that have been orphaned for 10 years. I used to pay very close attention to consumption at Maven Central for all the Java products. Very highly dependent upon projects with no committers, no activity. They don't fix any bugs. And people wouldn't know. So as we get a hard requirement from a bank saying, "You must have SBOMs; they must be comprehensive," the suppliers on that bank are going to have to move away from some of those that don't participate, but there's every opportunity and encouragement that people get better at this.

>> DUNCAN SPARROW: Thank you, Duncan Sparrow. So as you all know, I'm the one who's anal on the one-hop verse. I call it full tree because it's -- that's one dimension how far deep you go. The other dimension is this whole concept of you don't actually know what's beyond you. I'm using Josh's product, but I don't know what's in Josh's products. So I can just say Josh's product. I can't say more because I literally don't know it. So unknown is different, particularly from the consumer's viewpoint. Because part of the argument is - I'm going to use the medical device example because they're going to come up in the trial next. Is it the medical device manufacturers job to go and hop, at least to the extent they can, or is it the hospital's job to do a hop? In other words, if the device says, "I use Josh's stuff," is it the medical device's manufacturer's job to talk to Josh and get the more or is it the hospital's job to talk to Josh, get more? There's always the different dimension of you don't know what's out there and that's a

different issue. But just on completing it -- So my question for this document is, I know at least in the parts I wrote, I always assumed full hop. And I do agree with one hop is better than no hops, and three hops is better than two hops. And there's you know, I can't go beyond what I don't know, but if I can, -- so the more complete it is, the better. But do we have anything in there on the concept of the more complete it is, the better it is?

>> JOSH: I took a note on that. I think it's fair that we could show side-by-side or head=to-head because this is a Commerce Department voluntary multi-stakeholder process, my answer in this context is we could just talk about the relative benefits of both side-by-side. If you go sector-by-sector, for people who may use this process later, like a regulator, the one regulator is going to be here after lunch, expects it for the medical device maker going through premarket submissions or 5 10k changes to say what they're using on all the way down.

The hospital market demand will be a market force, in this case, a regulatory force in that narrow use case is asking the final goods assembler. In other parts of the world, though, take this away for physical supply chain. There's already case law and stuff for cars about the final goods assembly. That's why we use that word is that car makers are ultimately responsible if they choose a bad tire manufacturer because they chose it. Right. So that's the McPherson versus Buick from nineteen sixteen or seventeen or whatever. The final goods assemblers tend to be the accountability point. Yes, market demand could do that, but that's outside the scope of NTIA in this multi-seeker process. How it gets used -- I think what we're building is something that's useful and can scale and support lots of use cases. How it gets used in other sectors I think will emerge organically.

Art Manion. At the risk of repeating myself too much from the from the framing working groups point of view and not to disagree with Josh's point about Buick. The name of the thing that I've got in my hands is who I'm going to go after when something goes wrong and their choices are going to now come under question. The framing group sort of model is there's a least cost avoider component to this. And everyone does their little part. The thing works in theory very nicely, and that's really sort of the goal, so I don't want anyone to have to go back and push back hops farther than they have direct knowledge of. If everyone just manages what they produce and make SBOMs, what they produce and demands SBOMs for the supplies they get, there's this beautiful graph puzzle that goes together, and we have complete information. So that's the dream, my personal dream.

>> JOSH: And to ground this very recent example, I just had to patch a flaw in my product that was a third party component. I had a big fight with people. They said, "It's not our fault. That's a third party." I said, "It became our fault when we chose to depend on that third party component and our customers are going to scream at us, not that open source project."

So it's a matter of opinion. It's just the throat that's nearest to you to choke. And I vaguely mentioned the Buick versus McPherson, but as an example, that would be the Buick was the car. The Firestone tires, they were wooden, by the way. Wooden wheels were breaking and they sued Buick and Buick said, "It's not our fault. It's Firestone's." But the case rule is, as the final goods assembler you are in the best position to avoid risk in your complete, finished good. So that would have been, say, a compound part or singles apart, and we don't know what's going to happen with software. We're in new territory. But the notion of, "They're going to yell at me even though I depended on that third party library," or they're going to look to scream at the person for the thing they're consuming, whether it's a toy or something else. That's just my prediction of how that's going to play out. But yes, to your point, if everyone does their part, it becomes much easier to do the whole thing.

>> LES: So for we get to for in this today I do want, and this may sound elementary and it may -- and everybody here is like, "Duh," I'm sure. But I have gotten these comments outside of this group. And when you look at bill of materials and its definition usually means what's in there. But we've gotten -- I know you've probably built your own furniture from IKEA or something, but the bill of materials isn't wide. The comments I've gotten outside of here is, "Is an SBOM truly -- why are we just talking about deep?" So I want to make sure we keep talking about deep and levels that we want to make sure that everybody is on the same page or at least the way I see it is it's a matter of wide as well. So your bill of materials. It's all your software that you are actually including that may not be in IP. So I know it sounds elementary, but I have gotten comments. "Well, I'm just going to put you know -- will you look at this as those ten big items, not those 15 other little items?".

>> JOSH: Yet, again, picture in the future that the way we write software, the tools we use to compose them, is just self-describing. You're not doing like some harvesting thing and tasking a bunch of interns. Think of Java right now. To make a build, you have to know what you're building from. So there's already sort of an SBOMs in pom files, for example. So for these different ecosystems, imagine a world where the depth and breadth is a byproduct of making software. Now, that's a little bit North Star, and the reality is going to be difficult in between, but that's what we're trying to cause is a state where we have traceability throughout. Cars do it. And they do the physical parts. They know what every screw in every batch of screws from that supplier -- Legos have a little unique number, a little tiny piece of plastic that cost less than a penny each. They know exactly which dye and which cast and which position actually was defective. So that traceability exists; we can do the same with software.

>> JC: I think that there is a tendency to focus on open source components, which is valid because everyone uses them and we analyze them. It's important to also discuss in the bill of materials that there may be licensed proprietary components within that same piece of software, which happens as well often. And we should probably get in front of this idea of what happens when a manufacturer considers the presence of a proprietary license software library to be a trade secret, for instance. So a software bill of materials has to include everything that's in it, even though you would rather not disclose that this special secret thing is in it that you've bought.

>> JOSH: So I think -- this is not a complete satisfactory answer, but it has been covered in a lot of these working groups before. The way to compensate for some of the opaqueness of the 5 to 10% that is custom code or proprietary code is that the boundary becomes the final goods assembled has a version and an SBOM for it. So it is a trackable thing, and if there is a voluntarily disclosed against that combined thing with 90% transparency of open source projects and 10% of home-grown and handwritten stuff, the boundary of being able to do the triage on that is the completed versioned thing, a step just above what you're saying.

>> JC: So to follow that, what about -- I mean custom code is if you're in-house custom code, that's your IP. What if it's a third party dependency that is licensed? Yeah, sure, except for the stuff you've personally written.

>> BRUCE: You can assume they're all licensed. I mean, but it's possible to get one that's not licensed, but virtually all of them are Apache license or, you know, BSD license or something.

>> JC: Sometimes there is a product that is sold as a software component into your product.

>> BRUCE: Sure. That's a vendor that you pay for, and there can be free ones are not free ones.

>> JC:: Sure. But the point is at what point are you getting transparency out of the presence of those products in your product?

>> FRIEDMAN: I think some of that falls in the broader conversation. The ed case that I think you flagged earlier is sometimes the terms of use explicitly says you cannot disclose that you're using this. This gets to, I think, some of the broader questions we're going to talking about this afternoon, which -- getting into depth, getting into changing some of those norms. What's the short-term solution look like, which is something that Art talked about and that Kate's going to talk about, which is being very explicit about when we're not listing information, the known unknowns, and then the longer term solution, which is if you're using this stuff, that's on you to work with the supplier that you're already paying and have some kind of awareness for vulnerability management.

>> JOSH: Yeah. I think the short term answer my own words is we call it translucence or opacity like a known unknown. I think my hunch is over time people will tolerate fewer and fewer nodes in the tree that are opaque. I understand your use case and I can even think of a vendor that's doing that. I don't know if that practice will survive, but I haven't thought about that much.

>> JACOBSON: So I've heard that concern also that it's intellectual property, whether it's a trade secret or not, that it's considered intellectual property. And I believe the counter to that is really your use case of survival of the fittest.

>> JOSH: That's right.

>> JACOBSON: Right.

>> JOSH: Yes. There's current state and there's future state, and I think we're going to go through some growing pains. Also, by the way, some of the early people that said which components we use are proprietary to us and it's intellectual property, it was pretty easy to rebuff claim because many of those libraries they were using demand you acknowledge their use, and in fact, if you look on their websites, they're already acknowledged. So some of that was lobbyists spreading fud. Some of it is there's definitely terms of conditions and some high assurance use cases where people don't want to reveal the use of that. I think those things work out. To your point, as this gets more adopted, we'll have either accommodations for that or that practice will get squeezed. But a lot of the people who say this is proprietary intellectual property, I'm like, "Yes, it is - for the project that's giving it to you for free. It's not yours. It's theirs." And in fact, if you don't acknowledge it, people have faced lawsuits, and that's one of the first sets of software composition analysis products was to avoid lawsuits for people violating the terms and conditions of open source licenses. So those cases, a lot of those claims are fud, but not all fud, but we should be able to be adults and separate which ones are valid vs. scare tactics.

>> FRIEDMAN: If you were listening in on the phone, just a reminder that star one gets you in the question queue. I'm also keeping an eye on an email, so if you really want to watch the webcast rather than the phone, you can email me something, and I will try to get it to you timely.

>> JOSH: Ben and I did some edits back and forth pretty last minute, so that section also -- we're going to do a little bit more refinement on consistent tone and flow for the rest of the document, but there's some decent ideas in there. But that's really the area we'd love to invite you to focus on is which parts

are super-clear versus, more importantly, which parts are unclear, because we either going to cut those out or we're going to clarify them.

>> FRIEDMAN: All right. Any other comments, questions? Demands? All right. This group, again, similarly has evolved over the past 6 to 10 months, and I think they've found something that is both -- covers really important things to say as well as very useful things to say. I think all of these documents can be used in this, and I think is going to be very useful for the folks who need a little encouragement to see why this is useful. This document is going to very powerful.

>> ALLAN FRIEDMAN: Now we will talk about -- we talked about the what; we talked about the why; and now we'll talk a little bit about the how. So, Kate, can I ask you to come up here and we'll pull your slides up.

>> JC: All right. I'll try not to destroy any computers during this briefing.

All right, so. So some of the content in the standards and formats presentation you will have heard. Thank you for also being here. You'll have heard before. You know, we did a pretty good job of having our homework done on time. So this is sort of a bit of a capstone for us. We also do want to solicit feedback. We've gone through one set of solicitations, but we definitely want to get any last comments that people have on this. So afterwards, please look up the resources and give us comments.

So the agenda for our presentation, you know, basically what we've done and our summary of it. So our charter was very clear. It really had to do with, first of all, survey of the landscape, what exists, what is being used, whether it's commercial or open source. What are the initiatives that are underway, and how do we get to a survey and an analysis of what provides machine-readable data? Because it was very clear from the beginning, if it's not machine-readable, it's not automatable, and if it's not automatable, it's really kind of not real. From a security and an assurance perspective, because manual processes don't scale.

So investigate today's options. Start to map between those to understand what's out there, what the formats are that have in common, where they don't have commonalities. We explicitly acknowledge that this is not one solution to rule them all, that there are actually slightly different use cases with upstream and downstream for software bill of materials, and we need formats that accommodate that range of use cases, so it's not about finding the one, And to wit, how the solutions can work in harmony.

If there are different use cases for SBOMs and there's different formats that are in the sweet spot for those different use cases, how do they harmonize, as well as to reach out and look about what's available internationally, because there are efforts underway around the world in this domain, and we want sure that we've got everything on the radar.

So objectives. Success looks like machine readable format that provides direct linkages to both the components and the suppliers. So there's different terms that have been bandied about - publisher, project. Everything has been brought under this whole rubric of a supplier, whether it's a commercial or an open source project.

Things that can be signed, because in addition to the composition, there's issues associated with chain of custody. Where did it come from? How did it get here?

And that all of this be automatable, because there's just too much volume and velocity right now to make anything but automatable solutions viable. Again, we looked at both commercial and open source solutions. There was a bias towards lightweights, because in both the consumption and the production of software, there are entities large as well as many entities that are small that are not highly capitalized. And a lot of the vulnerability comes from those end tier suppliers.

So we want to be able to look at solutions that can disseminate throughout the supplier base and also things that can integrate into the software development process. So rather than being an afterthought, how can we look at solutions and formats that can be produced, again, automatically as an artifact of the software development process?

What's new in the white paper that we have? So we have some examples. We're very much favor of show rather than tell. And these are albeit toy examples, it's really important to have examples. And we've illustrated this example both in SPDX and SWID formats, and additional formats have been added to the survey as well as discussions of pluses and minuses of those formats. Contributor section has been added and the standard word-sniffing and formatting has been done.

So, Kate, do you want to talk about the example? Sure. This is.

>> KATE: This is the example that Art had. We just have not rotated around and we were looking at it from the perspective of what software coming in, and have included this one in the documentation. After we get everything consolidated and collaborated, we will update this as well.

But understanding what includes what was part of what the framing group determined as sort of a minimum viable. And so what we've got is this example in the document as well as SWID and as SPDX expressions of how to represent that in those formats. And everyone just open the document and so look at what it actually looks like. You should be able pick out the right elements pretty quickly. I didn't cut and paste it into here.

Other formats that have been raised. We've been hearing CycloneDX and InToto. So we're going to be adding that into the survey. And then the open question that asked for help from this group is, "Are there other formats that you guys are hearing that you want to see shown -- described in the survey and contrasted and compared?"

So I think we've got most of the ones we all know about at this point. But if there's anything missing, this is the right window to please let us know. And any comments or feedback about where we're missing things or reviews and comments be welcome at this point.

>> JC: Ok, so I think we're leaning into some potential next steps. One of them is a tooling survey.

>> MALE SPEAKER: So. Oh, sure.

>> JOSH: This is not -- I'm not campaigning for this, but I do hear a lot of supporters of this multi stakeholder process have started experimenting with CycloneDX, and it feels like early on we went SWID and SPX. I'm not saying we should revisit that. I'm just asking, you know, explicitly, is that one already planned to be in your comparative?

>> JC: I think we should basically keep the formats as a sort of living thing. We have [INDISCERNIBLE] format and CycloneDX, and there's going to be others. And so I think that we should -- it would probably be better to have that other formats as a kind of participatory thing where people could document them.

Yeah, we just have basically a small section at the end, at least have a mention in the way to look up more information about these formats. CycloneDX sort of an interesting one in the sense that it seems to be tracking what the framing group is doing and then iterating over time with it. And so it's a bit of an evolving one to -- sort of hard to sort of put a line in in the sand there right now.

>> JOSH: From our working group's perspective, and especially if we add the action item Duncan's requesting here, which is mapping which use cases are possible or better or best, there might be a material use case prohibited or unlocked by the presence or absence of something in their comparison.

>> JC: And I think that we also, as we move into this kind of tooling discussion about what's out there to produce these things, we also need to really take a look at what are the tolerances of these various formats at scale, because we've done a lot of testing of various formats of what does it mean for a system to produce one of these things from one pipeline, 100, 1,000, or 10,000. And there are some real limitations associated with things that were not built for scale from the get-go. Some of that's language limitations. And so for an enterprise that's just running -- developing one application and one pipeline, it may not really matter. But for enterprises that are running 600 pipelines 60 times a day, it may matter.

>> KATE: We do have various constituents that are operating at scale and we need to have something that will work that scale as well as be lightweight enough that individual, open source, upstream projects can actually apply things to. So we've got that whole spectrum here that has to come into play. Each of these formats was designed with various dimensions and capabilities in mind, and so it's basically mapping those dimensions and capabilities to the use cases is what's needed, I think still. But I'll take a note and we'll see if I can discuss that more. Any other questions?

So I guess a more of a note, I guess, than a question when it comes to this. I'm Mark Galpin with J. Frog.

So I guess from the perspective of companies like ours, I mean, if you look at the subject of SBOMs, there are a lot of tools that are effectively tasked with creating SBOMs today. I can tell you being one of said tools that we all basically use proprietary formats to express those. And of course, part of the reason we all use proprietary formats is because for a whole host of reasons, there isn't a well-accepted standard in the community of what we should be outputting on. And I guess from my perspective, we'll be perfectly happy in the event that there is a broad community acceptance that this is the standard they should be outputted on, setting aside quibbles that will then be had, whether various key pieces of metadata are or not included and sorting out those wonderful aspects of open standards, which we are still, I think, a ways away from getting to that type of discussion. But I think, in the meantime, I guess my question is what, if anything, are we doing in this sort of forum to sort of acknowledge the fact that, yes, vendors do exist that have these proprietary formats?

>> JC: I think that's very important. And I say this as another toolmaker with another proprietary format. I think the thing is when we look at all our formats, we're seeing a lot of the same things. So it's the jsons in a different order. And one of the things that we've discovered because we provide assurance for other people's products is that the format that you're in , ultimately, if you're producing all the data, changing the format is easy. It's whether you have the data to start with or not, that's the hard part, and lot of people don't.

>> JOSH: I agree 100%. That's why I said I'm not here to quibble about what should be in or should not be in the format.

>> JC: I think this is where the framing group has a real role to play and the use cases group has a real role to play in the sense of what can be accomplished in the presence of data, whatever format it's in, because the presence or absence or the ease of production of that data is such a higher mountain than putting it in a different format that getting to stage zero on a real industry level is just the hardest part,

and I think if people can understand what do I need to output, like how many levels down, stuff like that, we can take our requirements, .txt files and ruby gems and whatever, and we can we can converge on some formats. But understanding what has to be in those things or those things plus enhancements, I think that that's where I think all the vendors kind of have to sort of keep their eyes on the horizon.

>> MALE SPEAKER: Yeah. No. And I completely agree with that statement. I guess what I was looking for maybe in the document was -- I don't get the feeling that we're trying at this stage to invoke that convergence. I think I think it's coming, and like I said, I look forward to it.

>> KATE: So the start of that convergence happened when we started doing the translation between the different formats and what the framing group has come up with. There is actually a table in the document underneath the trends -- Table 1, actually, the translation harmonization guide where the fields from the two different formats express the field -- what's been identified to date so far from framing as what's important in a minimal SBOM.

>> MALE SPEAKER: Right.

>> KATE: It's there.

>> JC: And I would actually encourage, in the spirit of including more formats, but with some rigor, that new formats that are included have to go in this table, have to go into this mapping table of what's in it that's exactly the same as what is in these other things, and what is in it that's not the same, and what's it all called? Because if we don't have that table where we can say apples to apples to oranges to kiwis, then it's all just going to be, "My baby's prettier because they're my baby," and that doesn't really help anyone.

>> KATE: We also have a those proprietary -- for each individual format is expressed as APIs, and they're not versioned, and they change over time, and so as making things machine readable and consumable by others becomes a problem here.

>> JC: And just down the line to respond, if we have this all in the table, that actually gives us the precondition for the kind of SBOM decoder ring that it would be trivial to write.

>> MALE SPEAKER: Yes. Well, I guess basically that was that was the process question I was trying to ask.

>> FRIEDMAN: A really important process questions, so thank you. I want to go to Bruce and then Josh and then Duncan.

So we need a canonical format, and it might be one of the candidates wins SPDX SWID something, or it might be this document, but we should define what it is that's going to be our canonical format. If the framing document, great. Then let's say that. If it's not the framing document, then let's say what standard it is, and then we'll define the mapping from the canonical ones to all the other ones that are possible, and if you want to bring up a new candidate, part of your job is to define the mapping. It's not easy to map between these things, and as someone who's done these kinds of things before, and there's all kinds of things like direction, and we have long discussion already about directions. What is up versus down? And you'll have the same things there. People will think that when this is related to this, it's this direction or that direction. I mean, there's loads and loads of them. So, part of this, if we want to get adoption fast, we have to define the canonical format. I don't care if it's a standard or the framing document or some other document, but it has to be one.

>> JC: I think canonical is a really interesting word because it's from religion. And generally, it's good to stay away from religion when it comes to software. I think that we have identified some robust formats, and we've also suggested that there are others that we can map against them. How hard or easy it is to do that mapping, it really depends on the complexity of your data and the skill of your technical team. I mean, we've converted between three formats in a weekend and in meme compliant XML, so that's an exercise left for the reader.

>> FRIEDMAN: So continuing with the language term, I think process in this working group is set out to be ecumenical, exactly, because I don't think while there is -- there are pockets of use of all of the stuff. We are not in a world where there is a clear winner. And this is where I put on the government hat and say, "It's not the government's job to pick winners and losers," and I'm guessing that more than half of us have been involved in the standards fights before. And so I want to applaud this group for trying to sort of say, "Let's talk about how we get an SBOM in an automated model, and then we can move on from there from a tooling perspective and let the market decide. And I very much take your point of saying, "Let's have the standard model of what an SBOM is." I think the framing group which a lot of you have been participating in has done a very good job of that, and I think the standard group took that from the framing group.

>> JC: So these are our next set of deliverables.

Before we jump into the next set I want to make sure [INDISCERNIBLE].

>> JOSH: I just repeat myself in that graphic, in that beautiful purple graphic, we're all in a supply chain. Most of us are in the middle. So as someone in the middle, in a practical sense, my customers are asking for -- some of them are demanding SWID; some of them are demanding SPX. I'm going to produce both. Right. And if I get more CycloneDX, I'm going to produce the third one. Just like you can see in a lot of reporting things, export is a PDF, comma, separated files, XML. This will just be a presentation layer output if we have the data.

>> JC: Yeah, I think that --.

>> JOSH: If we have the data.

>> JC: Yeah. In Microsoft documents, you can now export I think eleven formats.

>> JOSH: Yeah. But on the other side I have tools that I need. So I went to them and said, "How are you going to support me taking your tool and producing these plural?" And they said, "We're going to produce all of them. We're just waiting to see --" I don't they should wait to see, but they're intending to give me the options for those as well. So as long as people can produce the data types both as me producing them to my demanding customers if I want their money in a free market and for the tool chains that I'm going to use to meet that requirement, I think it's going to be pluralistic for a little -- multilingual for a little while.

>> JC: Question over here?

>> DUNCAN SPARROW: So I have three questions that have sort of evolved through all the discussions that have come up since I my hand went up. The first is more substantive and the second is just two points of clarification. So the first one is: During the discussions on formats -- well, actually, I think it came up in all three groups, but I think it was the format group that got tagged with it. There was this issue of identifying the piece of software you were talking about and how to do that. One question is, did that get resolved, the whole whether we used -- I know there were three different three-letter acronyms, I don't even remember that we're talked about. So anyway, so the first question is: Did that get resolved, and is that in there or is that sort of just hand wave still? The second question is on Cyclone. There's a point of clarification on the CycloneDX. So the current document has one line in appendix that's literally says the word CycloneDX and there's literally no text under it. If I understood you right, the intent is just to put some text in there. Right? Not to put it in the table that you said it doesn't really count unless you're in the table. So I just wanted clarification on that. And third is: You made some comments about things not scaling. Was that a particular comment about you tried something with CycloneDX, or that was a generic, you know these two work, and you haven't tried it with other ones? Those are my three questions. Thank you.

>> KATE: Order backwards going. So, no experiments have been tried with CycloneDX. No one has stepped forward to do the work. OK. First off, someone has to step forward to do the work- - add the stuff in and prove it out. Most of this has been done by people who have been stepping forward, who are experts in their areas, and doing the work. We have not become experts in areas domains. Next question. Back.

>> JC: Yeah. I mean, to follow on, yes, more text about CycloneDX. That's easy. But when it comes to do the mapping, it kind of goes to Kate's point of view from CycloneDX is going to come forward and do the work to get that mapping into the table.

>> SPARROW: [INDISCERNIBLE] must remember, wasn't the inventor of CycloneDX, and in this room at the last meeting.

>> KATE: Yeah, and he's actually participating in adding question SPDX 2. So I think there's a reasonable collaboration emerging at the technical level. We are planning on putting a description of CycloneDX. If you actually looked at the Google doc, you'd see that's a work to be done, and we need to add InToto in, which is what we're commenting on. And so I'm looking for other formats that may need to be added so that we make sure we have a fairly complete survey of the landscape at this point.

And then your first question was sorry --.

>> JC: The naming.

>> KATE: So, yeah. So there's multiple approaches right now for identifying that software component out there. Software Heritage has IDs; CP has their identifiers; Pearl is there. And all of them have strengths and weaknesses. It came down to -- with a lot of discussions with the framing group that we needed the four elements that are listed in this table of the supplier, the component, and so forth. The component itself can be anything from a container to a package to a distro to a file, to a snippet.

>> JC: Or a repo.

So, it's sort of like a container could be like a directory even for that matter, or component can be a directory. Sorry. So we have use the term component because it has the ability to scale across those concepts.

>> JC: And I'll say I'm, more generally, as someone who deals in software logistics, not just software assurance, that when you get into this issue of naming, this is where two domains that are related but not the same touch each other. One is assurance. What do I know about the thing? And then the other is chain of custody, which is, where exactly did it come from? That particular copy of that particular file, how is it taken down, moved and delivered? So you have a concept of location and transportation that bumps into this "What's on the packing label?" And it's a very interesting discussion about how much of that does any customer want to know. When it comes to hardware, people are much more firm about their requirements that they want, the tracking of where the box is. With software, that discussion is not really mature. And there are very demanding customers, and then there are customers who have absolutely no chain of custody or care. And we're sorting that out.

>> SPARROW: Just a point of clarification, because in the health care, which we're going to hear from next, but in the health care trial and the previous present tape, last time they presented on it, they mentioned that was one of the issues. They had four versions of what a human could look at and go, "Oh, those are all the same thing." But people named them different. So I just -- how we're going to deal with that. is it punted or solved?

>> FRIEDMAN: And on one hand, you're right. It is a little hand waving. On the other hand, need to acknowledge that what you are attempting to do is provide something that works for as much of software as possible. That covers an enormous domain. Naming, we talked about this from the first meeting, is a known hard problem. I don't think we will --everyone has a solution, which is, "Everyone should just name things the way name things, and that works really well." I think the standards group, and thank you to everyone who participated in this group, and thank you to JC and Kate had a very hard problem, which is they had to try to talk about this in format world. Roll up your sleeves and build things, but at the same time, still trying to be as agnostic as possible about any particular solution, because as someone who runs these processes, everyone loves to say, "Oh, yeah, let's just slip my product in this government document that I can run around -- "

>> JC: And also, getting away from that, I mean, this sort of you get to this principle of verification, right, which is, How do I know that that thing that you call Acme version 1.4 is that thing that I can fetch down over there?" And as Allan said, it's a complicated technical issue.

>> FRIEDMAN: And we also have -- and I think just speak to that, that's why a lot of folks in the framing group really wanted to see hash as something that we can do. So there are a number of different options. All right. Do you want to do a very quick tease of what we're going to be talking about after lunch?

>> KATE: Well, so open questions have been coming back for us -- are, "OK. How do I use these formats? What's out there? What can I use today? What can I use --? What's in people's pipelines? What can I use today? So we'd like to try to see if we can get a survey of what's actually happening with these formats today and what tools are available for people to start to build into their CICD loops and -- .

>> JC: And also, I think that speak about different formats and different vendors and providers, I think this kind of quick start guide -- I would personally love to see -- OK. Here's a piece of software in a

repository somewhere that's open. Here's the tooling to produce the SWID tag. Here's a tooling to produce SPDX. Here's a jfrog. Here is a ion channel Siva. And then, people can essentially show and tell and get into a discussion about how it's used and what's good about it or whatever and where the mappings are.

>> KATE: That's where we'd sort of like to head towards. So I guess just to take us home is the initial goals we've had for this work group, I think we've pretty much come through the stage of achieving them.

The options are pretty much all investigated. We've documented them, and we've had a very explicit goal of acknowledging no single winner. And so I think we've kept to that.

>> JC: Yeah. And as things get more real and exemplars exist, I think that's where some smart person or people can probably take maybe two weekends and create, "Here's your decoder ring between these things," and just automate that, and then we'll be happy.

>> KATE: And so I think that's where we are. So if you guys have got any feedback in the next two weeks on the document, by September 15th, if you could send email to one of us or to the mail list or write it in the Google doc, we've got the link there, too. So whichever way is most convenient to you. Thanks.

>> JC: All right. Thank you.

>> ALLAN FRIEDMAN: All right. As you can see there, as Evelyn said this morning, "If this were easy, it would have been done." And I'm really impressed to see how we're doing. So now we talked about the what; we've talked about the why; talked about the how. And now there's the group that I sometimes referred to as the script -- we'll do it live, which is it came out of our first meeting a year ago where there was some frustration of people saying, "It can't be done; you can't do this."

And so I'm really happy that led by Jennings Aschi and Jim Jacobson -- Let's show that we can do this for our own little corner of the ecosystem and not as a pilot, not as a commitment, but as a let's just demonstrate that we can do as a proof of concept.

And Melinda, I'm going to ask you to open Jennings Aschi's. He's going to join in this presentation. And let me run over here and pull up your slides.

[SETTING UP SLIDES]

>> FRIEDMAN: And we've got Mike from New York Presbyterian as well to join this presentation.

>> JIM JACOBSON: All right. So you'll hear from me Jim Jacobsen, as well as Mike Dittemore from the NYP. So the goal here is to give a status update of where we are and where we are is basically the report that you saw the handout out. You saw outside as a handout and you, hopefully, have in your hands now, or on your computer now, but the status of that document is that it is content complete, format complete. It's available now for feedback and for final feedback based upon everyone's input. So if you have input, please send it to the mailing list. I would ask that it be two weeks minus a day, because we meet on Thursdays, and we want to be able to sum it all up by two weeks from now on Thursday. So it's based upon the feedback today and subsequent feedback.

So where did we start? We started with establishing our goal of a collaborative effort between manufacturers and health care providers to find a format that would work for us to communicate this information from one side to the other and show, by facts on the ground, that we could communicate the information and more importantly, that we could effectively exercise use cases against that information to show the utility of it.

So the result is that we did prove the effectiveness of SBOMs as a tool for transferring this information. This was information was useful, and it was information that has never been available to health care delivery organizations up until now. So it's a concept that works. We have a lot of bumps in the road in going through this proof of concept, because there was a lot when we started out that was not determined. But we took note of those technical issues, and we'll provide that information in our in the findings in the report. I mean, we have provided that information and the findings of the report.

So last time we were here, we talked about the fact that we had some observations, but we had not collected at all into specific findings. Today, we present the full findings of the proof of concept. And just a reminder of what we did include and what we didn't include - we used SWID and SPDX both formats. In almost all cases, manufacturers produced those in both formats. We tried to tackle the topic of dependencies, as you'll see in a little bit. That wasn't entirely successful, but we did take it within scope. We wanted to deliver this content over the internet and in a machine readable format. We excluded hardware At the time the FDA was concentrating on CBOM, a cybersecurity bill of materials which included the concept of hardware, but we did not feel that it would enhance the ability of the proof of concept to show effectiveness.

We did not include vulnerability information, although that was one of the topics that we considered. We didn't feel that that was the right level tool to identify the vulnerabilities.

Unique identifiers. We didn't want to tackle the naming issue, so we came up with a provisional way of dealing with that.

We didn't provide significantly the idea of, yes, this component's in here, but you don't have to worry about it because Z. And we didn't include an API to access the data.

So these are the number of use cases that we did explore. Initially, before we started with the proof of concept, we said, "What are the use cases for the proof of concept? But also what are these cases for using SBOMs for medical devices in general?".

And in consultation with the use case group, we identified seven use cases for procurement, and for asset management, we broke that down into three categories: general asset management, risk management, and vulnerability management. I'm not going to go through those numbers, but his is an example or a summary of the use cases that we will be talking about today of the findings that came out of the exercise of the proof of concept.

So with that, let's skip right to the findings, because that's the meat of what this report is all about. There's some overview in the report, some description of the use cases, but the real meat is the findings, and so that's what we really want to talk about today.

So first of all, we don't start off with the findings against this specific use cases because we also wanted to examine how easy or difficult it was to generate SBOMs and to ingest SBOMs. On the other side. So we looked at generation first, and we identified the fact that there was no automated process that that existed today, no tooling provided an end-to-end chain of generating an SBOM. So in many cases, there was some automation involved and some scripting involved and also manual process involved in generating a relatively small set of SBOMs.

The flexibility of SWID and SPDX, we said, was great, but with flexibility you get ambiguity. And so some of the what we had to do was create a specific interpretation of how we would use SWID and SPDX both in order to convey the information that we needed to. There was a lack of standardization for certain of the elements that we were communicating, component ID being principal among those. And I don't need to reiterate that; that's a well understood problem for everybody.

In order to get to the level of full automation, it would require being able to pull information from many different sources within the suppliers' environment. So in the case of medical devices, the information is represented often in many different sites with many different elements of the manufacturers operations - different business units, different ways of representing the data. And so that was a challenge, a challenge noted that we would have to overcome for full automation.

Dependency information was also challenging, and in just opening the kimono, there were there was some doubt amongst manufacturers about could this information actually be useful to the health care delivery organizations. And I would say we were unsuccessful in exercising this aspect of SBOMs because of the complexity of producing the information. It was a challenge that, eventually, we felt was not germane to proving that you could use this data rather than showing the complete tree at any point, because that was the challenge that we couldn't meet because of the reasons that we've all identified of creating a complete tree.

>> JOSHUA: Joshua, without completely stopping the flow, I want to come back to this because, as I said, we can claim it's difficult. No one asked me, not one of the participants. It's not an indictment. It's just I could have produced some. It would have had more things in it. Some of those are exploitable things that a hospital, if they saw that, would say, "Oh, I remember that attack. Yeah. That could have affected me. I would have liked that heads-up." So I hope it's not self-fulfilling, and I respect that Phase 1 was very tightly-scoped. But my bigger point is I hope it's not self-fulfilling, it's too hard, because had I been asked, I would have provided.

>> JACOBSON: Yeah. So we originally it included in scope, but felt that in order to get to that level, it wouldn't provide enough data about usefulness of SBOM information.

>> JOSHUA: Yeah. And I disagree with that. But I'd like to make the case offline.

>> JACOBSON: That's a perfectly legitimate position, but we were just trying to exercise the use cases, and none of the use cases depended upon that information being available. So it's maybe something that we work on in the future.

The device ID we've talked about, but -- I'm sorry component ID, we talked about, but the device ID, that is the end product that is being delivered to the HDO, there was no way to specify that within the SBOM. So that was communicated external to the SBOM, that there was an external file, like it read-me, basically, which it mapped that out, and maintaining SBOMs per software version was identified as something -- not something that was encountered during the proof of concept, because we limited the time frame for the proof of concept, so there wasn't a lot of change over time, but the aspect of maintaining multiple versions for an installed base, where you could have hundreds of products with dozens of versions, tens of versions, five versions, whatever it is that that becomes an increasingly large headache or potentially could be depending upon the infrastructure of the manufacturer or how many different versions they maintain in the field, et cetera, because these systems are not necessarily always updated. We often include or make available updates, but often they're not incorporated by the end user.

And so now we'll talk about consumption.

>> BRUCE: I had one comment here because it came up recently. Many times, the product developers don't actually know what version of a [INDISCERNIBLE] goes in because the creation of these picks the latest one at the time. And so if you create your software 10 minutes later, you might get something different. And the tools available, in many cases, don't keep track of what version actually came in. They just pick the latest. And that is something that needs to be considered in tooling or something like that. I know that one company, which people have heard of, Netflix, has changed their tooling, because none of the standard tools gave that information for them, but they are doing that today. And so this is an issue for versions, which you were just talking about, and the fact that people may not actually know what version is in there.

>> JC: Just a response to that particular point. That just grabbing the latest version, not having a lock file, is identified as bad practice, and there actually are CICD pipeline tools, including ours, and I'm sure lots of others, that will flag non-specified versions of dependencies as a fail state and break the build. So we

have commercial products in the marketplace that will actually preclude software building if that specific state exists. So if you have non-version dependencies and it's in a bill of materials, you can see where it's not specified, because there isn't a version specified because it's picking up the latest. That is, in fact, explicitly expressed in the software bill of materials with a non-provisional version, and you can flag that as a high-risk software bill of materials.

>> JACOBSON: All right. So next, we're going to take a look at the consumption or the ingestion of those bills of material, as well as the real findings from the use cases, the important stuff. And for that, I'm not going to speak to the important stuff. I'm going to leave that to Mike.

>> MIKE: Thank you, Jim. So to reiterate, the HDO's consumption analysis and ultimately the exercise of these use cases was successful, but certainly not without some challenges and areas for improvement. So I'll go through some of those. The first one. Perfect segue way from the previous presentation was the lack of a standard universal ID for this particular components. Without that, there was some manual intervention required, some human element to actually go into the SBOMs and make a determination as to what those particular components were. The HDOs did try to leverage some approximate searching or fuzzy logic to see if it would yield reasonable results based on that. But ultimately it was determined that doing so would not represent accurately exactly what those components were. So we highlighted it as one of the primary challenges, and a lot of the other challenges that we do have to kind of dovetail a bit off of that one or overlap a bit.

The second one, which certainly does, is that some manual correlation was necessary with and without some varying success. So in situations where it was pretty easily identifiable as to what that component was but didn't necessarily match across multiple SBOMs, we could say, "Well, it's either this or this," and then map that to a particular item that we were using from the national vulnerability database and then create a risk profile for that particular attribute. There were other situations as well where we weren't necessarily sure exactly what it was and had to maybe make an approximate guess or some type of assumption as to what that may be and then assign a risk rating to that as well.

The third one is that there was no authoritative end of life software database to automatically pull from, whereas we used the national vulnerability database and a feed from that to create something to kind of throw these attributes at and then return a result. There was nothing that had authoritative end of life dates or data that we could potentially pull from. So we had to do that somewhat manually.

The next one is custom software. So it wasn't reasonable to make the assumption that just because something wasn't found or couldn't be identified, that it could be custom software that was included as an attribute within the SBOM. As such, there was really no way, no flag or no particular item to say, "This is software that was custom developed and has been included as a software dependency in this SBOM. And as such, there was no way to correlate that to the overall risk profile of the device just due to its unavailability.

Another one was the lack of a patch level. So some of the more hefty or bulky components that would change drastically, the vulnerability and exploitability, would change drastically depending upon patch level had to be assessed manually. So there is no way to see, for instance, with the Windows OS, what KBs and patches were installed upon delivery. That had to be done separately and then maintained separately as well.

And lastly on these, the overall completeness was essentially accepted as is. There was no audit or validation done by the health care delivery organizations, so we had to have a reasonable level of trust between us and the MDMs to say, "This is not only accurate but also complete." We didn't do any type of gap analysis or actually take that and then look at the device and see if we could enumerate other things that were not particularly defined in the SBOM.

So some particular use cases, the procurement use case. Across the HDOs, we did not have anything that would automatically import this into procurement tools that we were using. Unanimously we did use a SIM to do that and write some custom scripts to get the data into there and then really use that as the data warehouse, so to say, or source of truth. As I said, compare that against something like the MVD, and then use that really as the central point, and any of the other systems would be calling upon that to identify those particular things.

Another one was the lack of a schema definition, an XSD. All of the HDOs essentially came to the same conclusion as to how to parse it out just based on the SWID or SPDX files that they got. But there was no actual definition file to just say, "Here's how you should do it.".

One of the things in the use cases were that, on the success side, were that device vulnerabilities could actually be quickly identified, assuming all of the challenges are addressed and we have an accurate and immutable name such as CBE or something like that.

Assuming you can get that in, you can go to something trusted as the national vulnerability database. You could easily make that correlation and generate a risk profile for that device both upon delivery and installation and over time as well. Subsequently to that, you could also, if vulnerabilities identified as part of procurement, look to necessary compensating controls to mitigate the vulnerability or exploitability of that. If you know there's a known vulnerability that's on a device and it's being introduced into your environment, you could look at something like network isolation or access control lists and firewalls to bring that in, but then mitigate that risk.

And then lastly, here, we do have one that says HDOs were unable to correlate some data with component end of life due to lack of readily available end of life information. It had to be done manually.

Second one is asset management. So the current implementation of the CMDBs of CDMS systems across the radios were unable in their current state to import or map the parsed SBOM data. It's not to say it. wouldn't be possible with some tooling or custom scripting. In fact, we, at Presbyterian, have worked with our vendor service now and kind of said, "Hey, this is something we'd like to actually explore," and their eyes started to open up wide, and it's certainly something that they said could be implemented so that the asset inventory could have this information available there as well.

As I said, customization or additional tooling could be done due to the timeline and scope of the proof of concept. It wasn't done, but in concept it would be successful.

And then, as I mentioned, after the PoC execution, there were some vendors that did express interest in moving forward with this, and we have had additional discussions around that to get that spun off.

Risk management use case. We didn't consume the SBOMs directly to any risk management or EGRC tools. Conceptually, though, it could be done as well as it is on machine readable. Similarly, the ongoing monitoring of devices wasn't done just due to the truncated timeline or short timeline, not necessarily truncated, but short timeline of the PoC, but it's certainly feasible. There's nothing to say why that wouldn't be feasible to do going forward. We were able to use the CVSS scores in the MVD to come up with qualitative data.

I know I think it's certainly been mentioned here in the past- vulnerability, exploitability, different things. So that qualitative number is certainly something that needs to be analyzed a bit further. In addition, even though some libraries may be exploitable, it could even go down to the method or function level that is actually being called or used. So it does kind of provide that surface profile or risk score, so to say, but additional analysis is likely needed. As with all the other use cases, a common thread here.

Lack of a naming convention certainly impeded the execution, full execution of this use case. And we did identify as configuration vulnerabilities as a gap. There's no real way to represent configuration vulnerabilities, so you can look just at the components and say, "Yes, no. Yes, no," but it may be contingent upon the specific configuration of that component that actually results in the exploitability or not.

And lastly, here is a vulnerability management. So the findings were essentially consistent with other use cases. I don't need to go in those with too much more detail.

Some things that were interesting were kind of the opportunity or potential for red and blue teaming exercises, surface view attack vectors. So to do some more focused and red blue team exercises within the health care delivery organizations that use unique attack vectors that we may not see all the time, and then, subsequently, developed defense plans against those, something the we're necessarily maybe not placing as much focus on. The SBOM, when presented to our vulnerability management teams, did not have an immediate or material impact on the way that their current practices were being performed. However, they did say that the risk profiles that were generated upon assessment of the SBOM could be paired alongside some vulnerability scanning results to create a more holistic view of that device.

And with that, I don't know if Jennings is on the phone.

>> JENNINGS: I am. Can you hear me?

>> MIKE: Yeah. Can you see the slides?

>> JENNINGS: I can.

>> MIKE: Wonderful.

>> JENNINGS: Well, the slides are actually -- the video is lagging a bit, so I'm probably just gonna wing it a little bit. First, I want to apologize for not being able to make it down. I had a little issue with the day job and had to head back to the hospital, so I apologize I'm not there.

I think just in terms of conclusion and next steps, a couple of things stand out for me. First, I just want to begin by saying this is not in our conclusion, but I agree with Josh that the dependencies are needed and would provide further insight. And I think it's a discussion we have to have and try to figure out how do we get from where we are to where we need to be. And this speaks to really the goal of this effort, which was let's just get this done. Let's make those up on the fly, if you will, a little bit, because there were discussions in health care about this for some time. There were groups in health care proposing health care specific SBOM formats, which was kind of loathsome. And so we wanted to basically contribute to the broader discussion within our industry vertical, but also be part of the cross industry discussion that occurred.

So I think in terms of just thinking about the ultimate findings of this, it's clear that SBOMs can be generated and consumed as it relates to medical devices and this is something that is viable. And ultimately, the FDA has proposed final guidance that would require this. I think that's a great step in the right direction in which to [INDISCERNIBLE] talk about how as an industry we would implement that, but the idea that this can't be consumed and doesn't provide value is I think something we should just take off the table right now. We had transparency we have not had before, and in terms of operations, I think we successfully realized many of the use cases, maybe not to their fullest potential, but those are things that we can tackle down the road.

The other thing that really stood out was that as we talked about this, speaking to a near Presbyterian experience with some of our key information security and technology partners, there was a real interest in this outside of just the people working in the PoC, and this speaks to really, I think, the next steps conversation. At the end of this, I think everyone who joined us Thursday calls realized we need to do a second PoC. We need to think about the lessons that were learned, incorporate those. We need to think and discuss this with the other working groups and think about what the requirements for this second PoC would be. And I think a key finding was we really need to think about the ecosystem of partners that would be necessary to make this real, and this speaks to the issues around automation and tooling on the MDM side. The discussion we've had all morning about just different aspects of the challenges with the current standards and opportunities that exist. And then on the healthcare delivery organization side, as Michael the saying, we have CMDC and [INDISCERNIBLE] vendors that are ready to step up and help with the ingestion and thinking about this is a feature for their customers in the healthcare space and obviously outside of that.

I mean, service now is not specific to healthcare, right. And so they're intrigued at the idea that they could be the repository for A customer from any industry vertical that leverages this. And I think one of the exciting aspects of the second PoC, that we've just kind of had high level conversations. Right. It's expanding this to more MDMs, more HDOs, and also ultimately involving other folks who are in this meeting and some of the other stakeholders and then folks like Splunk and InfoSec companies as an example. So there's nothing written in stone, nothing concrete. But I think we need to line up this PoC and start thinking about how do we expand this. And one thing that was even thrown on the table was expanding it outside of healthcare and having maybe another industry vertical or two joining and really trying to push the envelope on this and making it practical.

So I think just to wrap up my comments, I couldn't be happier with the participation, the collaboration, the fact that we showed that the goal of software transparency is not some fiction. It's something that's very doable. It doesn't mean that it's going to be easy to really operationalize this in a sustainable manner. And those are the sorts of challenges we need to think about next.

>> FRIEDMAN: Thank you, Dennis.

Any questions? We've got just a few minutes before a scheduled break?

>> DUNCAN SPARROW: Hi, this is Duncan. So three points. Number one dwarfs the other two by far. So thank you very much to both the hospitals and the medical device manufacturers who did this. This was a really lot of work. It made some very valuable findings. I'm going to nitpick on a couple of things, and I'm sure other people will, too. But the bigger picture is this was really good. I realize you had to go through a lot of policy issues. You had to go through a lot of legal issues that are just not fun to do. And it was just -- you should be applauded for the work.

Now, to nitpick pick a couple things. Josh had mentioned the point that, as a supplier, he didn't supply it. You said, "No. That was in your terms of reference. You guys decided to only go one level deep." That doesn't actually show up in your SWOT analysis, and so your slide sort of showed a couple of points that don't show up in your SWOT. And I just wondered if it could possibly be added or added to what you want to do next or something. But just it seems like verbally more came across and comes across in the paper. That's one point.

>> JACOBSON: Can I speak to your point separately? Otherwise, I'll forget.

>> SPARROW: Okay. Sure.

>> JACOBSON: So the question of the dependencies has come up and what we tried to do is make this as realistic and real life as possible. And so when we're reporting findings that the MDMs were being grumpy about dependencies, that's what's going to happen in the real world. And so what we have to do is prepare ourselves, prepare the arguments, to speak directly to these people that are wondering whether or not it has utility.

>> JENNINGS: Yeah. If I can comment too, I think one thing to keep in mind is that we really had a primary goal of showing this can get be practical and real. And there is going to be a lot of nitpicky things. We talked about that every Thursday, and we, first of all, really appreciate the nitpicky feedback, because we want incorporate that where it makes sense into the final documents. But this is thing that -- I'll think all good things in life happen through iteration, whether you're developing a recipe, technical standard, or a business process. And so our goal is to get this over the hump, so to speak, and tee up the questions for the next one, which I think is really where we are. So feel free to nitpick. I think we welcome that feedback and the dialogue as we move forward.

>> SPARROW: Thanks. And then my third point was, and I don't know if it's to you guys or more to one of the other working groups, and that's you mentioned the patch levels weren't available, which gets into the whole discussion of is version a version or is Virgin the version and patch is something more detailed. And so it's more a question for the framing group as to what defines version or maybe that's a this afternoon discussion. But it seems like that fact meant you didn't actually have the version, well at least I think of as the version, if you didn't have that the patch was in or not. So I don't know how to address that question because it sort of crosses three areas. But I do think that's an important finding because it matters that we somehow have to address things.

>> FRIEDMAN: Well, I think that's a great point. I think we can tie that back to the naming issue that I think we're going to talk briefly about after lunch. And just in the interest of time, I see that Josh has a hand.

>> JACOBSON: Know, just like you're getting a lot of nodding heads.

>> JOSHUA: There's a lot of onlookers and recordings and notes being taken, so just to overtly express, I have good, respectful relationships with managed device makers. I'm not beating them up. I'm merely saying for this system to work with that graphic we show, with that big sideways tree, upside down tree, right side up tree, whatever, we want to pick, for this to work, a basic primary assumption is for a final good assembler to meet the requirements of its procurer or regulator, they can't do it unless they also put pressure upstream, and I'm trying to, with empathy and understanding the scope of this, and I think Jennings and I are converging on this, it is useful, necessary, and valuable to start putting pressure on your upstream suppliers. And I was remarking not to beating one up, but if I haven't been asked, no one can claim they couldn't get it right. So I'm choosing to believe that I wasn't asked because of the scope of Phase 1, not that it's impossible to get, but that we chose not to ask yet. I would hate some of the critics of the SBOM process watching to conclude, "See, you'll never get it." And I want to be really, really careful in our language that we didn't ask for it, so therefore, "We didn't have it, and we don't yet know the value," is a different statement than, "We should start to ask for it, so that my upstream suppliers can be good suppliers to me."

>> JACOBSON: Right. And I think device manufacturers, in general, have criteria for their providers, their component suppliers. And it's important that this be one aspect of that. I would say it's probably very rare today.

>> SPARROW: And moreover, if I don't give it to you, I should lose your business. Right?

>> JACOBSON: Right.

>> FRIEDMAN: So it's a great segue way to flag what we wanted to next. But just very quickly, any last questions, comments? Again, two weeks minus a day to get to -- and again, I want to echo this comment that this is an incredibly solid effort. We've heard from a lot of folks that it's one thing to talk about something, but to actually build something, that's impressive. So thank you all. Great job to everyone involved. [APPLAUSE]

>> ALLAN FRIEDMAN: So. Thank you all for all that hard work. There still, as we've talked about, is some room for feedback in these documents on a flag.

A couple of things, as I've heard today, the sum of it, I think, is going to fit into what we might think of next steps, such as what does the process look like? How do we make this work in the marketplace? Something that I think I want to talk a little bit about after lunch is to revisit the naming issue, to see if there's more that we want to say now or if that's something that we want to say, "This is important. We know it's, in fact, a number of documents. Flag it as a hard problem." But is there more that, for example, the framing group can say about naming to highlight existing tools or something like that? Is there anything else that you heard today that you want to flag to discuss a little more about these documents?

>> MALE SPEAKER: One thing I want to think about is the configuration problem that you guys mentioned would not be able to detect [INDISCERNIBLE] from doing anything there.

>> FRIEDMAN: Configuration -- huge issue. I think that's going to fit in. And what I've got here is a set of potential next steps. And for those of you watching online, it's now linked to on the NTIA Web site. We didn't want to have it distract from the morning's conversation of said an initial list of potential next steps. And I think that's something that can go on this list. This is to start the conversation. I think there are too many things on these lists to easily do. But after lunch, we're going to talk about one. What does it take to get these versions, this phase, across the finish line? And we'll have a little bit of discussion about how you'd like to present them.

NTIA is somewhat limited by our content management system online, but there's some things that I think we can talk about and having suggestions from you will give me the ability to go to my coms team and my IT team to say, "Hey, we need a little more." But then, I really want to dive into sort of the next steps of extending and refining the model so it can put configuration on that too.

We've got tooling and processes. We can sort of bundle those together since one thing that's come up today is those very closely related, and case flag that one. The broader awareness and adoption case -- this starts to get into how do we think about this in the market perspective. Who are the partners that we need? Is it a role for government? Is there role for ISACS [sp?], things like that. And then, of course, the demonstrations - healthcare proof of concept too. Maybe someone else wants to take the lead in thinking about a proof of concept in their sector.

And since we know, as we've heard from folks like Jay Front, that people are doing this today. Let's start documenting where this has been done in a way that we can sort of show, "How this works," because there's a huge difference between an online project and a web app and a hospital medical device. And that's great. The spirit underlying is the same as we talk about these documents. Let's start talking about this.

So I'll leave these handouts just outside. For those watching online, we are going to reconvene at 1:15 sharp Eastern Time. Those of you in the room, if you're lucky, as you come in late from lunch, I'll thank you for joining by name. So that's their incentive to come and return to us on time.

Thank you again. We thought this was a really productive morning and really phenomenal work. So thank you all.

>> ALLAN FRIEDMAN: I would like to welcome everyone back from lunch. For those of you tuning in remotely, thanks for joining us again. We hope you had a nice snack as well. For this part of the discussion, we're going to ideally be a lot more engaging. And here is where we have to apologize for from the realities of technology. The webcast will be a little bit behind the live feed. And so if we're coming towards a topic that you want to actively participate in and you want to speak to us from the ceiling, then you may want to join the call bridge that is also on the NTI website. So as we continue this discussion, just think about how you'd like to participate. As always, you can send me an email if there's something you want to talk about, either during the meeting or afterwards. I try to keep an eye on things.

So this morning, I think I made quite a bit of progress, and it's helpful to take a look behind us and see just how far we've come in the year that we've been working on this. This genuinely has been a lot of really solid work. It's a hard problem, as I said this morning. We're trying to capture something that isn't just solving it for this sector or this platform. We're trying to create something that can be used across the entire software ecosystem from the most deviet of the dev ops web apps to some of the most old school embedded technology on which we all depend. And I think that vision is possible. And I heard that this morning. So what I want to talk about this afternoon is, revisit from the morning a few quick questions for these documents about our path forward on Phase 1. And then I want to turn our attention to the next phase. We might call it Phase 2.

There are a number of different next steps that we may want to move in. And there's for those you watching along, there's a list on the NTI web page called Initial Potential Next Steps. For those in the room, there's a nice little handy sheet. That's not meant to commit anyone to anything. Those are some of the ideas that we've heard from you over the last few months about where this could head and still open questions that you flagged that we want to tackle. So the first step we're going to do is figure out the gaps, what isn't on that list, and then we'll start to walk through how do we were famous list and ideally talk about how we can make some progress on that list. So diving into it. The one thing from this morning that came up is that naming is still hard. And it is something that we've heard on a number of meetings that there doesn't appear to be a single way to do it. Is this something that we think we can capture at least explicitly in maybe the framing documents? I know that these standards and formats document also says, "Hey, there's no perfect way to do it. Here are some of the existing ways." Or is that something that you see a role in the framing document?

>> ART MANION: I think the short answer is yes. We touch on it some now, but maybe not as clearly and directly as it needs to be. I think we kind of say naming is hard upon upon review of a bunch of existing standards and pointing to the SNF document. We think these four, five, six data attributes make up identity, but we don't actually say yes, 1, 3 and 5 are the required ones. It's it's some undefined yet combination of those of those things.

So that doesn't make for a clean way to do identity. But it's also a very messy problem. And I don't think we have the answer yet as to anything more specific. So I think the answer is-- short answer is yes, at least at least to more acknowledgement of that problem goes in there. I think further pilots or experiments, paper or otherwise, will be needed to poke around at, are our answers, our ideas any good there are not. So. Stop.

>> FRIEDMAN: Further thoughts.

>> DUNCAN SPARROW: Ok, so just point of clarification what I just said. So is it-- I don't think we're going to solve that problem at this meeting today. So presuming we don't solve it today, it's not going to be solved by the time the document comes out. So it's the intent to have the document, basically say, this is what we're going to work out next time or that we haven't solved it or what what's what's the intent? I don't think-- What I don't want to have happen is we ignore the issues. So you read the document, you can't tell it's there. But I also don't want to delay the document to solve the problem. So what are we going to do? I guess.

>> FRIEDMAN: One thing that's open-ended-- Go ahead.

>> BRUCE: The framework document-- I'm speaking for Art a little bit here -- does define a way to do naming. At least, it says you have to have these fields. Right? Now, what's in them isn't defined yet. I mean, you know, bits or something. But I think that it's-- I don't want anyone to think that it wasn't defined. It was defined. And more work needs to be done. And, personally, I think we need a directory of at least one thing, which is the supplier name. The supplier ID. The vendor ID. I don't know if everyone uses supplier yet, but we decide to use that because that's a better term. And anyway, that idea, I think has to be done. But that's my personal view and not the group's, but the group did define what the idea was, I thought.

>> FRIEDMAN: Something that's come up in the past four days. This isn't a random uncertainty. There are in most corners of the ecosystem, certain ways that we solve it this way over here and we use it this way in our package manager. So I think Federation could be a good approach. And Bruce, I know you've talked about the value of the Federation having some sort of an alias list as well as a potential path forward.

>> BRUCE: Yeah, this is part of the ID. I mean, and alias lists are needed, but we need at least one, and then and then we can have more, maybe.

>> JIM JACOBSON: Does it make sense in this case to be less agnostic? To use the religious terminology, more canonical in terms of specifying the either the content or the format here. Because if we don't get to some resolution, the problem could get worse than it is today.

>> MALE SPEAKER: And Allan and Art, I think there's some things that we learned in the the SBOM proof of concept that I think we can leverage as to how we approach some things for the naming. What kinds and what elements need to be provided. What you might be able to establish as a, quote, identifier for the thing being described. So I think we'd at least have some reference to fall back on this.

>> FRIEDMAN: Hang on a second. I want to go to Peter from Garmin, you're on the phone. Melinda, can we open up Peter's line?

[CROSS-TALK].

>> PETER: Hi, I'm sorry that the conversation moved ahead a little bit while I was waiting for my turn to speak. At Garmin, I've been doing a lot of the same as fund staff and also run into the naming challenge. The canonical name given by the supplier, and apologies for using that religious term again. What the supplier names, it does have some root in trademark law. So that's very good. Alternate names are also useful and corresponding identifiers. When there is a SWIT [phonetic] tag or a CPE or such, we've also

found that useful to include as alternates. But I'm happy to continue the conversation with you guys after this meeting.

>> FRIEDMAN: Fantastic. Thank you.

>> DUNCAN: Again, I'm not sure I got the answer to my question. I'm not trying to solve it here. I'm trying to determine what needs to go in the document so that we can complete the document versus what needs to go on the Phase 2 list? So we have work to do. That's a nice wanted. We all agree on that because I really do want to-- .

>> FRIEDMAN: Art?

>> MANION: Let me propose hopefully a shorter version of what I tried to say a minute ago. So I'm recently very familiar with the document. As of Monday evening, Tuesday morning, it is already addressed in there. I think it needs a little bit further, sort of direct. This is a hard problem. We're recommending the following. We are not going any further for this document. That gets this document done. We're willing to go this far. These fields, these attributes seem to be necessary part of naming. We're not exactly sure which ones yet. I think whether or not we state in the document, that is a further bit of work that has to happen. I'm very happy to have input from somebody who actually tried it, the Health Care Pilot to see what you're naming problem. I saw it show up. It came up. All of your slides had no naming you to pick from. So clearly that's a big problem. Anyway, that's the document answer. Right. Document. Answer.

>> FRIEDMAN: I'm sorry. Can you remind me?

>> MARK: I'm Mark from J.Crow. I was basically going to endorse the approach that was in the document, which basically says, this is still a hard, hard problem that hasn't been solved. I mean, I think, as we discussed, it's going to be some sort of federated solution on naming. But some sort of federated solution sort of predefined an assumption that says kind of this is what-- this is how you build even a federated solution. Right. These are kind of the core elements that will make up the resulting name. However, they're distributed in whatever other things have to go in within a certain technology or within a certain ecosystem or whatever, that I think it-- I know because I've given talks on it in various ecosystems. It is perfectly possible to stand up and speak for an hour on the subject of naming conventions on pretty much any technology you want to pick in this room. And therefore, I think it's perfectly reasonable to say that that's its own paper to talk about it.

>> FRIEDMAN: I'd say. NTIA is particularly familiar with the one example, I would argue, where we solved naming, which is DNS. And you may know that ICANN's annual budget runs in the tens of millions, which is a lot more than my budget.

>> JOSH: Just to foot stomp Bruce's point about aliases or also known as companies by other companies. They rebrand them. They even rebrand them when they didn't buy a company. So you will have plural aliases over time. So perhaps it's a more inclusive list of AKAs than it's a singular, definitive name.

>> FRIEDMAN: Great. Any last comments on this issue, otherwise our to-do item is going to be to have a little more attention paid to explicitly in the framing document. One explicitly say it's hard, but I think it already does.

>> FRIEDMAN: And then two, say here's the short term path forward of hit these fields. And so from those we should be able to derive most of the other ways that you can map between different naming conventions. All right. Anything else, anyone on the phone? For those of you who are listening on the phone. Star 1 gets you in the question and answer queue. Ok, so Duncan.

>> DUNCAN: Are we allowed to go to other potential topics from this one?

>> FRIEDMAN: Yes, other topics that were from the morning presentation.

>> DUNCAN: And again, maybe this is fully addressed enough in the existing documents, but at least it came up in the health care and, at least I know at times, it was a discussion point in framing the issue of the word that defines version combined with patches as opposed to some people think it's just version or whatever. Is that fully addressed at the moment? Or do we still have work to do on that? So when the health care people said we knew the version, but we didn't know the patch, is that just a terminology issue that they didn't use the same terminology that the framing group would have said, no, that means you didn't know the version.

>> JOSH: Yeah. We had a sidebar on this as we headed to lunch, which was in earlier meetings, we did differentiate between a versionable patch that, you know, could have its own unique hash in version number versus a hot fix or a backboard or we had a a language difference in definitions in earlier meetings. I think Rob Graham was one of the ones making that differentiation. I wonder if we'd benefit from avoiding plural uses the term patch, right? Just just for the purposes of our document, here's how we define patch. Here's how we define backport. Here's how we define hot-fix or whatever.

>> FRIEDMAN: And to that point, can we get some folks from the health care POC to sort of talk about how a cached version of a component would be different from a new version of that component?

>> MALE SPEAKER: Jonathan, when you see how we'd-- Are you thinking of, for example, in a medical device we may need to patch the Windows operating system so we're not touching anything on the proprietary software that we've created. But we're going to patch the Windows operating system. So are you referring more to that situation?

>> FRIEDMAN: And again, any Windows example from the desktop model that would then be a new version.

>> MALE SPEAKER: Well, typically with Windows, it's just going to have your base version plus of the 12 or 15 or whatever patches.

>> JOSH: But if you have a product, let's call your company Acme Medical Device. And you have 11.5 out there and you update your Windows underneath it, is that now not 11.5.1 or 11.6? Wouldn't you version that whole thing?

>> MALE SPEAKER: Historically, that's what's happened.

[CROSS-TALK].

>> MALE SPEAKER: it in a new book. But that's more historical. I mean, certainly, I think manufacturers are looking at more efficient ways to do patching when it comes to the OSes, etc. And therefore I think

some discussion amongst the manufacturers would be good too, to understand how each and every one might might treat it.

>> MALE SPEAKER: Just to throw a monkey wrench into this whole patching concept here and the SBOM. After a medical device vendor sells us the products, some of them even let us patch them ourselves with Windows updates. So then what happens to the S-bombs that we have been delivered from the vendor who doesn't know what we've patched? So how do we keep track of that?

>> FRIEDMAN: Reading Art's document, you're now the vendor. You're not the supplier.

[CROSS-TALK].

>> KATE: You get to you create the next SBOM.

>> FRIEDMAN: You have forked your supplier's product. There's an "r" in that word, by the way. I want to be very clear. Yes, one, two.

>> BRUCE: Go ahead.

>> MALE SPEAKER: I think another interesting aspect of that is how do you identify that patching in the SBOM itself? So you're using a version of Windows that's been released, such and such, it has a version number. You've got 12. How do I, as a manufacturer, include the information about the patching. Are they questions to ask and to resolve. Are those individual patching components?

>> JOSH: Well, I think it's also in his document, but it's a big, big compound part with the version number and a hash.

>> FRIEDMAN: So is that it?

>> KATE: I was just going to basically comment on how Debian and Ubuntu do it, which is they make it explicit that the patch has been applied. And they have the patches listed separately. A pristine start point there, [CROSS-TALK] the patch and then the sequencing.

>> MALE SPEAKER: So you've got to hierarchically-- [CROSS-TALK] does it become another hop? Because it's a next level of that base operating system, right?

>> BRUCE: So the patch really has to be treated like a different component, I think. And then it needs a relationship between that and whatever it's patching. So people understand that. And so, a patch really isn't like a patch in the sense of something else. It's a new component. And then you say, OK, my build materials changed. It now has this new component, which is this patch. And it has this relationship to this product. Version though, the way that they're usually used, is it needs to go forward. Maybe within it. You know, they might fork, but they seem to go forward and they don't have, this happens before this, or you can't, you know, whereas patches, you can pick different collections of different orders and include them or not.

>> FRIEDMAN: So the framing document has a set of when do we update the SBOM. And it includes when we've changed an underlying version. Can we have another section in there explicitly on patches?

>> MANION: Another thorny problem. Sure. Pending time and some effort. I want to say, though, this has come up at almost every meeting, I think, and it's still clearly unresolved and that's perfectly fine. I believe what the framing document has in it may not be clear enough, does cover these situations. And it could be that the patch is a new component I add to my list of components or that the patched thing itself becomes a new component. I think both of those or either are possibly OK. And what I'll suggest is, you know, if we had some pictures of what I'm thinking of is here's a very average tree. We already have the pictures with the agreed upon Acme Software and Bob's browser. If we have one of those, one of those with a patch, one of those with a new component, that might help us all figure out how I handled the situation, right? I'll agree. It's not well-defined yet, but it's also pretty squishy. So I think for the sake the document, we'll probably try to be little more clear about it. But I think it is unsolved. And again, I'd really like to hear from the health care folks how well or poorly that part went. But I think on paper, it's it's it's achievable, at least.

>> FRIEDMAN: Bruce.

>> BRUCE: One comment on that is, if you have 10 patches outstanding and they're independent and you want to make a new version, you have a awful lot of new versions. So you really need to treat, I think-- you really need to treat them as separate and just from a practical point of view. But that's just my view as a comment on which way to go in that.

>> FRIEDMAN: So I ask a follow up question, which is the use of the SBOM. So now, in addition to looking for what's in there, you also need to look, if you're trying to do this for vulnerability management, you need a tool that will verify what isn't in there, right? My tool says I should be using a version. I should be using a component that has these patches. Is that right? And like my characterizing that properly?

>> JOSH: I mean, to that point, if you recall the simplest use case we said at the very first meeting for Sam Sam ransomware hit Hollywood Presbyterian Hospital. Simply knowing you have the JBoss product in some subset of your devices, lets you go from 20,000 devices to maybe 200. Knowing that that flaw only affects a certain range of JBoss versions, lets you maybe take it from 220. So even knowing the presence of the project is actionable for our most basic vulnerability management. Am I affected? Where am I affected? It gets better as we get more precise because vulnerabilities cleave or match up to versions and version ranges. So this is just in the fine points of how much do I narrow that tunnel from 20,000, you know, 20 or 30 based on how we articulate a patch. So let's not say this is a deal breaker. It's a refinement.

>> FRIEDMAN: Good. Thank you. I think that's that's a good way of characterizing. Any further thoughts on this question of a patch as different from the version? Yes.

>> LORI: I would go to the comment that the patches could be maintained separately from the software. So you might have a like a base product which evolves on its own. And then you have set the patches, which you always have to apply as it's happening in the Debian world. It happens all the time. And in this sense, I would I would actually put them in the same category as, for example, compile options, which is, I guess, it's not yet been in this discussion so focused yet. But if you want to do vulnerability management, that this will be actually a very important option. And then in the same way, you should be having information about the base softer than the what kind of modifications are being applied to that. And that includes both the batches and also compile options in a way. So that would be a meaningful way of managing it from the [INDISCERNIBLE] perspective I see

[INAUDIBLE]

>> LORI: It should be different. There will be a critical difference. For example, if you use a stat guarding or canaries or not, and so forth.

>> KATE: [CROSS-TALK] The patches were already applied.

>> MALE SPEAKER: It should it should be thought of the information somewhere and probably maintain separately from the software itself.

>> KATE: In some sense, this is all starting to head towards a concept that's out there. Complete corresponding source type of information, which is all the pieces you need to be to reproduce the build effectively.

>> FRIEDMAN: And reproducible build is a lovely direction to head in, but still something that looks pretty far off.

>> MALE SPEAKER: So the compiler options is one of the things we talk about in the pedigree area. So it has a logical place, whether it has to be as pedigree, field, or whatever we decide to call it. But yeah, that level of detail is definitely part of what anyone who really wants to know how their software is going to behave needs.

>> FRIEDMAN: Doug.

>> DOUG: So I was just going to say following the previous comment, Bob said part of it, but now I want to hitch on slightly differently. Is this does get into the area of the Annex 2 of the use-case document, which I assume will be on the future work list that we want to actually work on that. But it also ties in with another point that came up this morning that we haven't touched on, so maybe we can lump them altogether, which is configuration. So sort of patches, configuration, providence, pedigree. It's all in a next-time lump, right?

>> FRIEDMAN: Yes. So again, we're getting really commendatore, very quickly. If you want to go in to config management, there is 20 years of reproducible build research and we will wander into that territory later.

>> JOSH: Not sure where this fits on the agenda, but just a point of order, in case you we're running low on time. We had a bunch of questions for the FDA representative who is now here. So one of the unresolved things from this morning is how far deep for that?

>> FRIEDMAN: No, I think from

[CROSS-TALK].

>> FRIEDMAN: That document says-- look, we're pretty clear on the documents. This is the bare minimum. So we're going to move forward on the sort of the next step.

>> JOSH: There is nothing for him.

>> FRIEDMAN: Do you need run-away?

>> JOSH: If it comes up later? That's fine.

>> FRIEDMAN: It'll come up later.

>> [INAUDIBLE].

>> FRIEDMAN: I want to focus on the documents that we talked about this morning. So further questions. Yes?

>> [INAUDIBLE]

>> FRIEDMAN: Correct.

>> DOUG: So we agreed in the format's group there'd be no winners or there wouldn't be a single winner. So we pick two winners and three or four runners-up in the back. Is the whole, what's the name of it Cyclone DX? Is that a to-do item to discuss? Is that a next-time work item? Where did that end up? I guess.

>> FRIEDMAN: So that discussion after 20 or so minutes said the goal is cross compatibility. And if someone comes forward, they said they were-- I thought they were pretty clear. Saying someone comes forward and says, here's the field mapping. We'll put it in. That's the field mapping is the priority. Did anyone get anything different from what was said this morning? Yes.

>> DOUG: So just to be clear. So if I gave them change table 1 and add this column with Cyclone DX is this field that uses this, this and this, it goes in or I got the impression there was more to it.

>> MALE SPEAKER: I got the impression they had two weeks to do it and I nudged for Steven to bring it to do it take.

>> FRIEDMAN: Kate? Thoughts on this.

So we are revisiting the discussion from this morning to say for table mapping, where the goal was to sort of make sure that we've got cross compatibility.

>> KATE: Right.

>> FRIEDMAN: And so if someone in the next week, because two weeks is not enough time for the group to do its work. If someone in this spends this weekend writing out more rows for that table, sorry, more columns for that table.

>> KATE: If someone wants to write more rows for the table, that's great. I think we're missing the relationship, though, in Cyclone DX. I think that's the moving piece right now. From the canonical definition that the framing group gave.

>> MALE SPEAKER: I mean, that what I got out of it was that people could add new standards anytime they felt like it.

>> KATE: Right.

>> FRIEDMAN: Yes.

>> KATE: Yeah. And that's fine.

>> MALE SPEAKER: And Cyclone, just a-- Cyclone deals with relationships by direct nesting. So it's a little bit it's more kind of natively XML than the way that Twitter XPS handle it for what it's worth.

>> MALE SPEAKER: Can handle, yes or no?

>> MALE SPEAKER: Yes, it can be done, but it just that conceptually it's different. That's why it looks like it's missing.

>> FRIEDMAN: So we have the folks who, I want it to make clear, if folks come forward at the very last minute again-- I'm very happy to have this discussion. But at the same time, we've been-- Those are the two standards that have been talked about for for quite some time. So, yes, it'll be great. But I also want to keep in mind that we want to get these documents in Phase 1. Further comments on the list

[INAUDIBLE].

>> FRIEDMAN: Thank you, tree direction. I agree that this is something that we should probably all talk about things the same way. I don't know we're going to resolve it on its merits. Are there folks who have something that can help us appreciate how they view this?

>> MALE SPEAKER: I think what we need is a tree mapping table.

[LAUGHING]

>> MALE SPEAKER: Clearly, we need another picture entirely. The tree's not doing it.

>> FRIEDMAN: More visual representations.

>> MALE SPEAKER: More trees.

>> FRIEDMAN: We'll get the metaphor right eventually.

>> MALE SPEAKER: Well, we've done up and down and we've done left. So I guess we should pick right?

[LAUGHING]

>> FRIEDMAN: Yes.

>> MALE SPEAKER: So we keep using a lot of metaphors upstream and downstream. And then we put a picture of a tree in its place because that's clearly the stream we were trying to tackle. So picking a metaphor would be a good first step.

>> MALE SPEAKER: I think I'm hearing a river system then.

>> MALE SPEAKER: Right.

>> MALE SPEAKER: All right. Yeah, I mean, tributaries. Right.

>> FRIEDMAN: And just to play off the note that you said I'm someone who always liked the root of the tree at the top of the page, because that's how I'm used to thinking about directed basically graphs. Art brought up the point that you just highlighted, which is we talk about upstream and downstream are pretty unambiguous in the supply chain. And so it makes sense to have higher in the tree, the upstream. That is one way of thinking about the orientation of the tree.

>> MANION: Not to beat us toon hard to death. The graph works no matter what. The graph mathematically doesn't care as long as the legend goes the right way. That's not the problem here. It's more, are we going to confuse people who are seeing the word recursive and nested and wondering what we're talking about for the first time and looking at the graph and being confused? That's where the metaphor could be helpful. And I want to not confuse them right off. Every map has a north.

>> MANION: So we could just say which one's north. Right. Well, north is up.

>> FRIEDMAN: So, you know, an NCAA-style bracket could be an option.

>> DOUG: So I still think for upstream and downstream, right to left us is better. But I've never seen a graph that had a funnel the way you guys do it. But I think you'll be more confusing the way you have it. But more importantly, maybe we should stop using the word tree and just keep it as a graph. And I think usually in graphs when you have one node and end nodes, the one's always on the top and ends always on the bottom.

>> MANION: So it comes down to we have a sort of a wide audience, I guess we've been trying to accommodate or reach so we can say graph and that has a perfectly good meaning and it's fine. But if people aren't glomming on to that, that's why we're saying river, tree, something else, right?

>> DOUG: So I guess a further point about that then. So we have a software bill of materials. Do we have experience to fill a-- Field of build materials has been around a long time and has a lot of work. How do they draw it? However, they draw it, let's do it. Let's not make software be different.

>> FRIEDMAN: Fair point. We will go and seek that out. Did you have a comment, Josh? Brenden, you had a comment.

>> BRENDEN: You were just to somewhat to cut the Gordian knot in half. If we're going to pick one of these three incompatible representations, I think since we're going to confuse significant groups of people no matter what, I think we go with the left to right interface because everybody looks at left or right and knows that, oh, good. This group made up their own definition of words and it makes it easier for everyone to just start. Everybody thinks they know how a tree works. As it turns out, we have many

different ways of incompatible thinking about how the trees work. So I would throw my weight behind what Josh's group outlined.

[INAUDIBLE]

>> BRENDEN: Also true. They had better graphic design and the other teams.

>> FRIEDMAN: All right. Any further thoughts? This is the last time we will talk about this today on the left to right idea. Further thoughts from the documents this morning, that we talked about. Things that were flagged. We've got most of the things on my list. A lot of the other ones, on services of best practice, depth, things like that. Clearly a next step, a practices and awareness and adoption story. So the next thing worth spending just a little bit of time on is, how we would like to share these documents. We've had this conversation now for the last few meetings of free standing versus tightly bundled versus loosely coupled. And it is my sense that the emphasis has sort of been loosely coupled. Seems like the path that I've heard a lot of people talk about, but I think it'd be useful to talk about that for a little bit if anyone has some thoughts about how they see these documents being shared and used and consumed.

>> DOUG: I vote as little change as possible so that we could get them out sooner rather than later.

>> FRIEDMAN: Thank you. I like that. Correct. So as it currently stands, they reference each other. We'll make sure that the references are all lined up. A number of folks have done some de-conflict. And as you read through, we can make sure that none of them blatantly contradict each other. I think the definitions have been well aligned thanks to some folks between health care and framing. And so now any any further thoughts on how we cluster these together? So now we have the question of presentation. So some of it's easy. They can all be in one document then four separate documents. We can add those options together. Many of you have made some comments about the NTIA Web site. So right now. What's happened to those [SPEAKING INAUDIBLY TO SELF]. Those got closed. That's unfortunate. So let me give you-- This is the NTIA self aware transparency website, which you can see is basically a reverse ledger, right? It's basically just a whole bunch of stuff that we're doing keeping track. Probably not the best thing to send someone to if we're trying to say, "hey, check out these documents here." I'll give you an example of what a previous NTIA project did. Still using our less-than-stellar content management system, but sort of has a "hey, here's some documents. Here's a very short paragraph about them. Here's the link." That's one option of something that could exist and then we'll have some of the process information below. Are there other ways in the short run? I can't promise that we'll magically have a really great web team by the end of the month. But our web team works hard and they are responsive. And so are there things that you would like or can envision about how you'd like these documents out there?

>> MALE SPEAKER: Can we have a diagonal dodecahedron?

>> FRIEDMAN: Three dimensional holographic.

>> MALE SPEAKER: A tactile experience.

>> DOUG: So under the vision side of it as opposed to the practical, this weak side of it. Would you at least consider something like putting it in markdown language on GitHub as a publicly available, stays

forever? And more importantly, you don't have to do all the work people could do pull requests. If you want to make it look prettier, put in a pull requests.

>> FRIEDMAN: So let's put that on the next phase style page. I think these are still-- we have documents. And if the document, someone goes and says, "oh, I think SBOM should be this." that's great.

>> KATE: One of the things that we do in another group is, all of the guides, the set guides to do for the open-source program offices, and they're all up on GitHub and issues are pulled there as well. As you say, I think it works fairly well for keeping documents working over time as needed. So I second that request.

>> FRIEDMAN: Yes, Jim.

>> JACOBSON: So I think what it will be used as is two things. One is a link to specific documents and a link to a place where I can get the set of documents. So anything that satisfies that would be sufficient, such as that.

>> MALE SPEAKER: I was just going to comment. We have three distinct documents or four. There's nothing that's pulling it together like a small intro that's probably couple of pages. And then link it to everything else.

>> FRIEDMAN: Right. Yep. Having a short overview could be very useful. That's something that I can work with some folks to draft and then circulate. And in fact, I'm guessing there's language in many of your documents today. That is that high level overview that could be very powerful. Thank you. Good suggestion. Other thoughts on just sort of saying, "Hey, we want PDFs. How do we get them?" And what would be useful for the people that you would want to communicate to?

>> JOSH: It's a little orthogonal, what we're currently describing but people were looking for what's every deliverable out of each working group. And it was kind of hard to find in a consistent tree or something like that. Like we had a PowerPoint for each working group each time we met here. But finding them very easily, hierarchically or chronologically, even if they're not the final product, there's still some valuable stuff in there.

>> FRIEDMAN: So making sure that we have the archive of all of the things that you've done to document the process.

>> JOSH: That's right. Yes, right.

>> FRIEDMAN: Great. That's a good suggestion. Further thoughts on how do we share the outcomes of this?

>> DOUG: So just point of clarification. So this is an NTIA multi stakeholder group. What is the status of the outcomes of this week? In other words, we're we're creating documents. They exist. Is there? Is it sort of the NTIA says this is now mine and they put it out or it's just, hey, we made this in a meeting and we're done or because that might affect how we presented what it what it is we're actually talking about.

>> FRIEDMAN: So the term used, if you pop back to the Stakeholder-Drafted Documents with some idea of when they were finalized. Each document contains either some information about the process that was used or links to another document that documents that. We keep it on the NTIA.gov website, but make it very clear that it is not and it is not a government publication. But it is. And my colleague Louise has actually spent a little bit of time trying to understand the legal status of that. But the short of it is, that anyone can pick it up, use it, share it, etc. The last question I'm going to ask you is, in addition to having four documents with a little blurb and a little overview blurb, useful to also have a Frankenstein, PDF, that someone can just say, "here's all of them" or is that something that is you don't need? I see some nods. I see some hedges? I don't want to make the case for Frankenstein's monster.

[INAUDIBLE].

>> FRIEDMAN: Is there a reason to not have that as another edition? Bob?

>> BOB: I was going to have a different point.

>> FRIEDMAN: OK.

>> MALE SPEAKER: It's harder to find what you're looking for.

>> FRIEDMAN: Good.

>> MALE SPEAKER: One reason for not having it, is it just work somebody has got to do so. That's going to delay everything.

>> FRIEDMAN: Fair

[INAUDIBLE]

>> FRIEDMAN: It is basically just like [INDISCERNIBLE] and SBOM, having all of them together. Anyone feel strongly one way or the other?

[INAUDIBLE]

>> FRIEDMAN: Yes, there are four components and so is there anyone who, when they think about how they would use these documents, thinks that would be easier to have a single link versus four links or just want to cite a single file versus four files? They'll be on one link.

>> MANION: Are we talking about both being an option or not?

>> FRIEDMAN: Yeah.

>> MANION: Sure. Okay. If it's both. Problem solved.

>> FRIEDMAN: Right. All right. So that's most of the presentation stuff I've got. Bob?

>> MALE SPEAKER: Could use a word. Presentations. I'd like to see something up there about presentations, about the effort. You've done one or two. If other people had things to donate. Because if I'm going to go talk to people. I'd like that to start with a blank sheet of paper.

>> FRIEDMAN: And I think we're going to slop that into the next steps discussion. All right. So everyone take a nice deep breath. We now have a path. We're not at the finish line, but we can see the end of lap 1, which is these documents polished. We all have our marching orders and we have our timelines to get them a little more smooth and finalized. I'll be working with all the working groups to think about this presentation layer. And making sure that folks who are new to the process can still get information, things like that. So now we get to turn to the fun side of things, which is what comes next. I've heard a number of ideas from folks really for the last several meetings about other things that we want to do that weren't captured in the work that we wanted to get done. There are four broad buckets here that I've tried to characterize. They're not perfect buckets. Moreover, they don't easily map to the established working group structures. Some of them do. Some of them don't. And so what I'd like to start off by doing is saying what isn't on this list. So Bob just talked about, you know, let's collect presentations and other documents, so that could be a very powerful thing to sort of say. Here's some of the writing that we've got here, stuff that that is around us.

>> KATE: It's in the same line as presentations. But is there some way of having effectively a gold deck for people who are trying to evangelize this in their own communities that they can pull off of?

>> FRIEDMAN: I'd like the idea of having sort of a shared deck. The challenge I would have with that is. How do we get community approval about speaking on behalf of it? So it's one thing to say I'm going to pull from the slides that came from each working group, but let's put that on the list of things to think about. The Gold Dec idea. Yeah, we can just have these as individual bullets. Emily?

>> FEMALE SPEAKER: I was wondering. I'm a little late to this discussion, but I'm wondering, is there already some thinking around who are the strategic pockets where you wish to have engagement be extra strong? And how to prioritize who you're speaking with in those arenas?

>> FRIEDMAN: That's a great question. I think what you've reminded me is I have handed out a piece of paper, but I didn't sort of do a quick walkthrough of it. So I'm going to take a moment and do a quick walkthrough, because almost all of these ideas that I've heard from various experts in this field and all of you over the over the past few months. So. Take a step back, extending and refining the model. So there are some big unknowns that we still have in terms of the what is the SBOM approach? How do we share the data? So what does that look like? Sometimes it's fairly straightforward. SWIT tags, followed binaries. Other times it's clearly not. And so need to think through what that universe can look like. The high assurance stuff that sort of spelled out. We've got sort of some basic assurance in the framing document with integrity and hashes, but there's certainly a lot of work to do and that can go very far into a high assurance computing. SBOMs for things that aren't on prem. Most of what we've talked about has been embedded or on prem. Very few people stand up and give speeches and say the future of software is on-prem software. So what are the use cases and what needs to change or how do we need to think about this for cloud, SAS, containerized, all of the fun, slightly different buckets that we have for software moving forward. And then the last one I have that some folks have mentioned repeatedly, and we really need a better name for this, is communicating non-exploitability of vulnerable components. So yes, I'm using open SSH, but I'm only using the PRMG, so I'm simply never calling that code. And I've also done some basic testing to show that it's not vulnerable. So let me communicated downstream so it doesn't light up people's dashboards. So that's the two figures to finish.

>> DOUG: I think it's artificially narrowing the current phrasing because it may not be about exploitability. It might be other postures such as these mitigating trolls in configuration options. I think the exploitability is way too specific. So if we get abstract that I can help later, but the way we've captured it is too specific.

>> FRIEDMAN: You were good with picking names. Do you have a--

>> JOSH: I've been have it "the disposition" I think was the phrase I've been using. But it's not well thought through.

>> MALE SPEAKER: >> We've been using context.

>> FRIEDMAN: Context. That covers a lot. Bruce do you have something.

>> BRUCE: I like disposition.

>> FRIEDMAN: Disposition, because then that means, you don't have to do anything. You have to apply this patches, mitigation or something.

>> BRUCE: Yes. It's better than what I've referred to it as "don't worry your pretty little head field."

>> MANION: The current framing document mentions twice in different places, but consistently it says exploitability or exposure. Those are the words it uses currently. But it's a pretty, pretty light treatment. We don't get into it in detail. Just that's the current word.

>> FRIEDMAN: Disposition or exposure. We will. As the folks, whoever is tackling that issue, that will be one of the first things that sort of figured out. So those are all in the two fingers. Two fingers. Yeah

[INAUDIBLE].

>> FRIEDMAN: If it is something that is directly relevant. Not to unpack. Not to drive the discussion further, but to clarify sometime directly relevant. So this is one finger on a point. Two fingers, is this a directly relevant to what's going on. Yes.

[INAUDIBLE]

>> FRIEDMAN: Yes, that is that is the plan. I'm going to go through the whole documents first. So as you-- If I come up with something that you want to clarify, that's the two. Tooling and the version online is being extended to tooling processes that you have two fingers up.

>> LORI: Yeah, I heard about the extending and refining the model. Is there a place for discussing doing the more abstractation? For example, this company that implements this protocol. But the other way around that this is needed for this work and we have these discussion.

>> FRIEDMAN: Firstly, process question is we're going to we're going to add to the list after we walked through it.

>> LORI: OK.

>> FRIEDMAN: But yes, that's something that, in fact, was in an earlier graphic where they said, oh, this this component implements this thing so we will carry that forward. So tooling and the the version that is now online says, tooling and processes, because they're sort of something we want to tie together. So one of them is what tools exist today for generating SBOM data and for consuming SBOM data? What further tools are needed? Which is a very big, expansive question that is going to be highly context dependent. And then there could be a time to sort of also say, hey, are there operational lessons that we can carry forward more explicitly from folks that are doing this either directly in the proof of concept or other examples? So that's what I've tried to bucket into the tooling and processing side of this.

>> BRUCE: Can you add the services to tooling?

>> FRIEDMAN: Tooling processes and services?

>> BRUCE: Well, I was trying to clarify.

[CROSS-TALK]

>> FRIEDMAN: Sorry.

>> BRUCE: I thought tooling might have meant services. And that's why I asked.

>> FRIEDMAN: So next, bucket awareness and adoption. This is sort of the how do we get this out into the world? This gets back to the comment that Emily said, hey, should we have a broader strategy to think this through? Then there's sort of or sector-specific or technology specific outreaches. So once we prioritize that, what does that look like? What are venues that we should be engaging? Are there champions that should come from someone who's going to go off into this community and be the evangelist in that community? Model contract language is something that a lot of folks talk about. How do I ask for an SBOM from my suppliers? What does that look like? How precise do I need to be? What's a lightweight way of doing it? What's what gives me what I need to do? Something that's come up in a couple of the working group calls is the value of having a FAQ, or F-A-Q, depending on your butchering of the language. So that's another area where I can imagine having the-- So you've just gotten started to this as you read these documents here, something that can go along with it. Here are the common questions. Is this a road map for the attack or things like that. And then the fourth bucket is sort of the demonstrations. I'm sorry, Kate.

>> KATE: In terms of awareness and adoptions, do we also want to add translations, since we're international?

>> FRIEDMAN: Yep, and we're going to we're going to add more. We're going to have the Gap analysis in just a moment. Sorry, I'm trying to walk through. So demonstrations, which is one, the proof of concept 2.0 to potentially further proof of concepts in other sectors. And then in addition to exercises which require lots of work.

We know that there are folks out there that are doing this today. And so can we engage in some documentation or solicit case studies, things like that? So, again, this is a lot of work. This is sort of the broad vision. Everything that I've heard, I've tried to capture. But even that's not enough because there are lots of great ideas in this room. So on the awareness and adoption side, there are translations. Yes.

>> DOUG: Ones that are missing here, is now the time to bring it up?

>> FRIEDMAN: Now is the time to bring them up.

>> DOUG: All right. So I think you're missing three in the first section. At least that we discussed this morning since I didn't see them on there. So one is further work on naming or whatever we're going to do there. Another one is the value of complete or whatever the words are going to be for this whole how complete, how transparent or opaque you make beyond the first level. That issue, I think, needs more work. And then the whole discussion we had both this afternoon and this morning version, slash, patch, slash, update, slash, config slash, etc.

>> FRIEDMAN: And I think. some of those are sort of naturally the same constituency and some of them, I think, for example, the depth question almost might be in an awareness and adoption story as well, because different markets are going to want to think about it differently.

>> DOUG: I just wanted somewhere on the list. That's all.

>> FRIEDMAN: All right. This is now your chance. Other things that are missing. We had translations. Laurie, you had a --.

>> LORI: Abstractization. So, for example, the component is required for [INDISCERNIBLE] let's saying that's so he could basically switch out components easily in the process. When you when you are holding your abilities, that would be going into the extending refining model part, I guess.

>> FRIEDMAN: Oh, interesting. So specification of what the component is doing?

>> LORI: And why it's actually necessary in this part. It is probably not really required component, but it would definitely help people to solve like the problems that are occurring in the ecosystem.

>> FRIEDMAN: That's a really interesting idea. Thank you. Yes.

[INAUDIBLE].

>> FRIEDMAN: Let's put that in the extending and refining the model, which we would call that maybe implementing or specifications. Would [INDISCERNIBLE] Exactly. Bruce?

>> BRUCE: I think we need to have a use case specific items to add to what's in the scoping document. I mean, sorry that the framework document now. So today, what's in there is-- everybody needs us and now we need to go to the next step. Refinement step, I guess, to say, OK, for this application, I'll just call that word. I know the words are in discussion. You need these fields. And this is this is the definition of that. And step one is probably define which cases we're going to cover. And then step two is what are the columns like all column for the statement that are needed and what is their definition.

>> FRIEDMAN: Do you have some examples in mind?

>> BRUCE: Vulnerability management is one, obviously, since that's been coming up a lot, but other people have ideas of what they want and you know, which which might be handling licenses, which is distinct. And is probably the most common one used right now, is for people doing SBOMs, as far as I know.

>> MALE SPEAKER: I was mainly pointing at the FDA when he was asking for it, when he asked for sector-specific ones, since we had a sector sitting in the room. [CROSS-TALK]

>> FRIEDMAN: All right. Seth, you've now been invoked twice. [LAUGHING]

>> SETH: How many fingers is that? What am I supposed to say?

>> FRIEDMAN: So we've talked a little about depth.

>> SETH: Yeah.

>> FRIEDMAN: And I know that you have thought a little bit about what you're going to be looking for. For those who don't know, Seth works for the FDA. Tell them 20 seconds of background. Please stick to background.

>> SETH: Yeah. So I work at the FDA, as you said, the Center for Devices and Radiological Health. We've been on the forefront of getting policy together for the Medical Device Manufacturers, but also working within the health care sector at large. I happen to be principally involved in the pre-market policy that we're currently revising right now. That has SBOM. I'll call them, they're not requirements per say. So I'll defer to my legal colleagues. But what it is that we need to manage risk. We can call them recommendations, but that's that's what we're working on. So I have some thoughts about depth. We're actually working on an issue right now. So just to use the use case that that makes a lot of sense in terms of how do we answer the question of depth. VX works, our real-time operating system was just I forget how long ago was essentially vulnerable and I had a lot of conversations in around Def Con about, you know, oh, we're talking about medical device manufacturers and others. Hey, am I vulnerable now? No, we don't use VX works. You don't use that particular version. Well, actually it's a subcomponents of VX works that's actually vulnerable. So what we have here is if we don't get the right depth and we create a situation where we have false negatives and in the field that I come from, which is health care, false negatives are usually bad. So not only was it a subcomponents, but the subcomponent was sold to other [INDISCERNIBLE] vendors as well. So this actually impacts other real-time operating systems. So if you're only looking for VX works, if you're only doing that level, you're going to miss a bunch of stuff. And I just don't think that's a-- I understand where we're starting. But this is not acceptable to miss things. So how deep do we have to go? Well, we have to go as deep as we need to define the vulnerability, which is why the tooling question for me becomes very important. I can dig a ditch by hand for sure, and I've done both. I prefer the excavator. They're fun. So I'd love to have more discussions around that. But we need to go as deep as we need to.

>> MANION: Great example. I mean, there were, I don't know how many conversations at Def Con I've had that were all SBOM problems. All these law-management were problems that are multi-vendor are didn't go back far enough to realize that-- And it Bruce's point about aliases, right. This specific example, Lib was the name of the library. No, not that far back, but the company that when River acquired at some point had a different name sold to more than one River, when River bought them up. So you have

an aliasing problem for your product name and for the company name, supplier name. Anyway, it's classic and everyone is just like that. If it's a multi-vender issue. So you need depth. Period. Yeah.

>> SETH: And honestly, it's a use case that I have to spend cycles on right now to deal with. And it's difficult. So can we come up with something that solves that or begins to work on that?

>> SETH: That'd be great.

>> MALE SPEAKER: I'd really like to not do anything right. [CROSS-TALK]

>> FRIEDMAN: Does anyone have a two finger comment on this? On Seth's remarks?

>> DOUG: So just a point of clarification. So the FDA has requested going full depth. We have as a group as agreed. We're coming up with tools that could go one, could go full. We're not going to say how far to go. How do we in Phase 2 and next steps? Not today. Today we are where we're at. I'm not proposing to change a single document we have, but for phase 2, how do we show the value of going deeper? My guess is the point we need to somehow get on our list.

>> JOSH: I'll bridge this two finger to the priority finger. Over lunch, it's not a great idea, but maybe someone will improve this idea of it over lunch. I said, you know, what might help is if we just saw a couple of attacks that have happened last year or two that could have been handled with one being greater than zero. But most of them are two or three or four. Then people say, I remember that attack. It might just be painfully obvious how much extra value you get by going further so that may not be a heavy lift. But if someone has a better idea, just concrete examples. VX works is one recent one. And the other part was I think it was your name, Emily? To to her point, earlier on, we may have had our sequence wrong. I thought our sequence was right, but we started in the use cases working group doing interviews of success stories which are now calling Phase 2.

So we have a bunch started there in a document called Sticky Notes. They're incredibly detailed. And one of the things I told the whole team early on is different sectors. So I think this is to your point. Different sectors have different nouns and verbs for the exact same thing. So acquisition for the Pentagon is the same as procurement for a bank. And what I had envisioned and we even recorded a sample of this is if we pick these ambassadors, could someone do a five minute or less intro primer or explainer video on the table we made that uses the nouns and verbs for that sector? Right. Very familiar. Nice on ramp. And then they will read the big document. But then I thought. I'm not saying we get to sign up to put videos on the NTIA website, but I do believe that some of this is a translation issue. And if we create that localized language, I think our adoption awareness would go way up.

>> FRIEDMAN: I like that, so we'll put in the adoption awareness side of things. Multimedia or multimedia and original or non-white paper communication.

>> MALE SPEAKER: Also specific sectors.

>> FRIEDMAN: That's good.

Yes. One and then two.

>> MALE SPEAKER: Now that we talked about VX's worst IP net vulnerability, can you do a case study like that to show how we could deep enough to answer some difficult problem? Address the FDA concern.

>> FRIEDMAN: I like that. Some case studies to show what are the obstacles of going deep and what are some of the tools and things that you have at our disposal today?

>> MALE SPEAKER: The VX works and subcomponents stuff started making my head do noodle things too, and I was thinking of all of the embedded devices that I've seen where they have started with, let's just say Red Hat Linux, and by the time they got it embedded on the device had jettisoned so much stuff from it to make it fit. But they still say it's Red Hat Linux, but I'm looking at it going kind of Red Hat Linux.

All the vulnerabilities won't apply to it because it's not-- I'd have to go component, part by part. The same thing happens with Microsoft's new IoT operating system. You choose which components you want to have in it. But if you just list Microsoft IoT OS, I don't know what that means. So is the SBOM able to address that the way we've conceived of it right now?

>> FRIEDMAN: So I think this gets-- Go ahead, Bruce. You've got a finger.

>> BRUCE: I think that we need a component removed for cases like you're talking about. I brought in Red Hat Linux when I took out a whole bunch of stuff. Here's what's left. This is really common. And I think that's that's something we need to look at.

>> MALE SPEAKER: Okay. Okay, Jim.

>> KATE: And just to your point about our Wind River. Wind River actually puts there SBOM for the Linux version publicly available and it takes it right down to the file level. So you have everything that's in Wind River Linux listed as a component. And then if you drill down, you can download each of those components for SBOM that they use to put the image together. And that's sitting there publicly today using the SPDX format. And you can have it in spreadsheet if you want it instead of a tag value. So, yeah.

>> FRIEDMAN: Yes. On the left, on the remove components option, Jim.

>> JACOBSON: Yeah. So how is removing components different from the open SSL case where you just don't use the components?

I agree completely. I think it is at the top level, it's this issue of disposition or context or exploitability. But we can I think that it's in front of you, is do you want to be even more clear. You want to draw a distinction between saying, I'm not calling that code versus that code isn't near here. Duncan, two finger on this issue.

>> DOUG: So back to that that discussion. I do think people over trivialize the Appendix 2 of the use cases. Only the federal governments who do a nuclear launch codes cares about all that assurance stuff. Everything we just said is all covered if you actually do all that assurance stuff. So my view is it makes that particular component that we need to follow that much more important, because it's those kind of problems that they've been worrying about, about the nuclear launch codes. But turns out that applies to everything.

>> FRIEDMAN: So, do what we want to drill down on that and sort of start to say how?

>> DOUG: I just want to say, I want everyone to not sort of just blow off the oh, it's just Bob and the government stuff when you do all that assurance stuff. It actually addresses all these issues that we need to do that.

>> FRIEDMAN: The telecommunications sector is already doing it, not in SBOM model, but they just do -- they have a very refined pipeline model that they can say exactly what's in it. It's not an SBOM. Further -- yes, Lori.

>> LORI: I have kind of a little bit follow-up on this in regards of how big is the appetite for actually developing a rudimentary maturity model? So you don't really need to be 1 and 0. It's more like a how far are you in regard to, for example, providing the next -- like a recursive information? Do you have services which would be able to provide the further follow-up? How fast are you able to do the patches? Do you have contact addresses for certain abuse or certain or whatever? So that's that's kind of like if this should be somehow involved in inside the SBOM or should it be referencing the SBOM? How it is interacting? That's up in the discussion. But basically based on that, you could start assessing your supply chain again. How big is that [INDISCERNIBLE]

>> KATE: Can I respond to that? So there's actually a program for open source projects, not necessary for companies, but that open source projects can go in and self-assess, self-certify, and basically put the evidence publicly and then raise a badge level passing. It was started from the core infrastructure initiative. So as the CII badging, and you couldn't find that type of information and so certain projects are basically attested a lot of things that you've been talking about already publicly, and so someone can go and look at it in a transparent fashion.

>> FRIEDMAN: Brenden.

>> BRENDEN: I'd like to go back a little bit to the question from a minutes ago of should there be a way to indicate to remove components. I think it's really interesting, and I'd like to say, "Absolutely not," because if you're taking components out that weren't indicatable in the SBOM some other way, that means the SBOM's improperly -- it's not granular enough, and at the risk of channeling my inner Richard Stallman, God help us all, it's not [INDISCERNIBLE] Enterprise Linux. It's not one thing. It's GNU Linux and it's 50 other things on top of it, and so you should be able to say. "This is all this stuff, and take this out," and this happens all the time in the web context, like g query is no longer one thing. Bootstrap is no longer one thing. It's 50 components and they're individually includible and they're individually specifiable.

>> FRIEDMAN: All right. And I think that point is very well taken. I saw some nods. And also, I think at least in the short-run, it is a subset of the disposition idea that if we can use this to communicate downstream, it doesn't matter if you have something less than the full component because compilers read there; things are being stripped out left and right all the time. But the important thing is to be as clear as possible if you know that something is being affected. Yes.

>> MALE SPEAKER: This is maybe we haven't talked about this, I think, the interface is JAVA data sets like MVD and whatever not. Do you have a map of that? Is there a proposed map?

>> FRIEDMAN: I think that's something that we didn't talk about quite enough on the naming side of things. On one hand, we want to solve the naming side of things, but on the other hand, the value of a

name is not just that we have uniqueness. The value of the name is that it's a key to other databases. And so I think that's a good point. Is that something I know we sort of closed Phase 1, but is that something that is worth making sure that we include in one of the other documents that we already have?

>> MALE SPEAKER: It's mentioned in, but not -- just very lightly. It's in there. It's the framing doc.

>> FRIEDMAN: Thank you. I think that's going to help folks, especially as they're making decisions. How do I pick a name? One of the goals is making sure that it can map to MVD and other things.

>> DUNCAN: But to his point, I think he was suggesting there was another bullet to add to your future work item on how to link to other things like licensing, database, and vulnerabilities is a further work item study. So I didn't see any typing when people said anything, that's why I'm asking.

>> FRIEDMAN: So let's make sure that we have that, and we'll do some further refinement of this list, both now in this discussion and then afterwards.

>> JOSH: You did some early binding on his naming point, but I think part of this for Phase 2 we should do is there are some potential implications on other institutions like MVD. So, for example, Art knows this, but some of us did a critique where there's a really heavy bias in MVD towards commercial enterprise-grade software and a real dearth of CBEs for open source projects. And some analysis has been done. And some of our friends in DHS that sponsor that Miter program have made some strides there. But as we do more SBOMing, it becomes increasingly important. So we should have some interlock and some conversations. I'm looking at one of my friends. We should talk about, as we're more dependent on CEDs, because I'm in my day job, I'm fixing a lot of flaws in open source projects that have no CDE, and there's a lot other people that are vulnerable because I fixed it, but no one else knows. So can we add to that list proper interlocks with institutions like MVD?

>> FRIEDMAN: I like that. Duncan?

>> DUNCAN: This question to Josh on that. So I thought the process was if you discovered something like that,that you reported it. There's not a CV. Didn't you report it?

>> JOSH: I'm working with. So someone reported to me. I found out its flaw in open source projects that never disclosed. So it's now a multi-party disclosure with Art, so that there isn't an accidental emergency.

>> BRUCE: There's a there's a clarification here. CVEs are supposed to be issued only by the supplier of the software. So if he finds a vulnerability in a third party's piece of software that he doesn't support, then he doesn't get to make a CVE. And then if it's -

[CROSS-TALK]

>> BRUCE: And then he's supposed to go to Miter, and then Miter makes a decision and they try to coerce e the guy to do it or whatever, but something happens.

But the other problem is people that don't understand this whole how to get CVs at all, if they find things, there's no good way for them to report them right now. So there's kind of two aspects.

>> FRIEDMAN: If only we had some DVE experts in the room.

>> MALE SPEAKER: So just just for clarity though --

>> KATIE TRIMBLE: So I actually run the CVE program. So I'm Katie Trimble. I run the CVE program for a Department of Homeland Security. In fact, I run all of the vulnerability programs for the Department of Homeland Security. So, MVD, I run that, too. So within the CVE database, yes, you are mostly correct, but you can go to Miter if there is not a known vendor CVE naming authority or numbering authority that can issue that CVE, or if the CNA is not willing to issue a CVE for it, you can go to a Miter and Miter will issue a CV for it is a legitimate vulnerability, or you can come to Art, or you can come directly to DHS. I am I see the numbering authority myself. I can issue you a CVE.

>> FRIEDMAN: Great. With this without the --

>> BRUCE: Oh, sorry. Yeah, I didn't know if the entire process. I knew the part about we're only supposed to issue, CVEs for our own stuff. We go to Miter if we can't figure out or something like that. But further that, I could go to you or -- all right. I didn't know in the past.

>> KATIE TRIMBLE: So that's a that's a failure on our part to communicate the program effectively. And we're trying to make an effort to be better about communicating and marketing ourselves so that some of this confusion is not so prevalent throughout the ecosystem. So that's my fault.

>> FRIEDMAN: And we can make sure that anything that comes out of us on this topic links heavily to all of those great resources that are being produced. Yes. Les.

>> LES: Yes. So feel free to throw stones and heckle me because I missed the last 40 minutes, in case you talked about this. But I did want to touch quick on that this case study for the demonstrating value of deeper level of SBOMs. One point I would make was would in this case data or whatever we end up trying to do here, is there a way we can figure out end of life? Because what I've had a lot of problems with is, and this goes to the configuration that was mentioned earlier, is we have people say, "Windows 7 is going end of life," but then so I'm not going to buy anything and I'll do anything. Oh, my God, you've got a vulnerable product. That's not always the case. Right. So there are things you turn off, things you don't do, things you don't use, things that aren't right. At some point it may be vulnerable, but it isn't on January 15th or whatever the date is.

>> FRIEDMAN: There are a couple of things in there. One of them gets back to this question of exploitability or context. And the other one, which you've touched on, I've heard from other folks, is, "Is there's some work that we can do under the auspices of this to make end of life components more visible in public?" and that was end of support. But, Art?

>> MANION: Very briefly, so clearly end of life is a concern, especially for longer-lived physical devices that outlast the software support lifecycle. Nothing that I'm aware of in the SBOM discussions is going to magically create that data, though. You're going to have yet to ask your supplier to give you an EOL date. It may be in a standard way or maybe it's integrated with the SBOM in some way, but without some of those dates, we can't get make them up or anything. So obviously, I guess, but yeah.

>> DUNCAN: Not to solve the problem, but again, end of licenses -- Multiple times, I haven't seen EOL typed on the screen, so just for future work items. Oh, there it is. Got it.

[LAUGHTER]

>> FRIEDMAN: All right. Other things and again, this is this is sort of the the wish list section. This is the stuff that you want other people to work on. Then we'll dive into, "What are you going to do?" Bruce, then Duncan.

>> BRUCE: We get to go through these discussions over and over again. It would be good if there was documents that kind of documented why the decisions were made. There were companions to the ones that we're making right now, so that new people on the project, and we're always trying to get new people, could read about them and not have to go through it again.

>> FRIEDMAN: Is this something that we can sort of put in FAQ wide of things, where --

>> BRUCE: That's a fine place.

>> FRIEDMAN: Duncan.

>> DUNCAN: So on the point of encouraging other trials or whatever, how are you going to pick besides health care, which again is wonderful that they are doing the POC they did, ow are we going to get other POCs involved? Is there a process? Is there just somebody here is going to raise their hand to say, "Hey - I'm going to do something"?

>> FRIEDMAN: That's exactly how this works.

>> DUNCAN: OK

>> FRIEDMAN: It is a voluntary process. Josh.

>> JOSH: You have a high level section for it. You called it under extending; you called it use of SBOMs or cloud SAS containers. I'm aware of some draft questionnaire stuff in Europe for cloud audit type things like, DE SBOM? I guess this is a Phase 2 thing, but I just want to add to that the idea that these more modern or host of things, it's more like an API to interrogate the current state of something, and there's some versioning thing. So I don't know if it's an entire working group, but there's certainly -- there are existing thoughts and existing artifacts we could at least collect. We've been postponing it in this room, but there are some materials we could at least collect that I know of.

>> FRIEDMAN: I think that's great, and that fits not just into that, but it fits into what does transparency look like as well as sort of the example you're talking about in Europe. I think this sort of fits into the e-model contract language side of things of how do you ask for this. And in this model contract, we can also add that sort of audit or things like that, other business processes that you can have to have that conversation.

Other things. Duncan.

>> DUNCAN: So Josh had mentioned before the issue of in the health care POC. because of the way they define the terms of reference of only going one level deep, no one actually asked him for his SBOM. It also got mentioned this morning how in the ideal world it would be great for both the medical device manufacturers and the FDA if the value of doing this in a standard way, somehow we could show that. So I know is a whole volunteer effort. We've got to get somebody to volunteer. So I'm trying to come up with ways we could entice someone to volunteer to participate, not from health care in the next version of the POC. So putting Josh on the spot some, given you know your stuff, at least theoretically, and you know that your components are used in medical devices, is there any way, PTC, so asking you as your corporation could entice any of its customers that you have known overlap with, that medical device manufacturers use X and this IOT device uses X. Can we get this IOT device to use to be part of the trial? Because then there'd be a -- they're not just two disjointed, "Hey, two random sectors that trial." It's actually, "No look. See this is the same dot." We can draw the picture that they have in the framing document that has that one consumer with the two parts on it. You could actually have a real one.

>> JOSH: So it's naturally cross-sector. Yeah. I mean, let me see. I understand your point. But some that left the room, I mean, I got a little clarification from Seth, which is we're going to have to go further back than one, but at least for that sector of healthcare. But I get your point about a cross-sector inverse ecosystem. Yeah.

>> FRIEDMAN: Are there things on this list that we've talked about that you want to unpack a little bit more? We've talked a lot about -- now, let's go to Kate.

>> JOSH: I think the notion of putting use cases is out there, but also use cases for showing success and showing how people are doing it and making it so it's bite-sizable and people can see an example of it being done. I'm finding cases where people are doing it today and highlighting -- and asking them to be visible about it.

>> FRIEDMAN: I think that's great. And we've got it under the demonstration section here. But I think it's also an awareness and adoption piece.

>> JOSH: Did anybody remember that sticky notes thing that Ben and I painstakingly interviewed people? So there's several of these in a Google doc that you can look at right now. And we thought about doing those short recordings with some of those people, but they use their own nouns and verbs. They identify their sector; they identify their title. So I totally agree we could do more. I just don't want anyone to think there are some --.

>> KATE: Just put them into some format where they're consumable. Other than it's taking it and making it so people find it and look at it. Look for it. Sorry. I'll go look.

>> JOSH: Is that findable or readable?

>> FRIEDMAN: Consumable.

>> KATE: Consumable.

>> FRIEDMAN: All right, Duncan.

>> DUNCAN: So I guess I assumed, so correct me if I'm wrong, but I assumed under awareness adoption when you have sector-specific and technology-specific outreach and potential venues and champions, I assumed that included making sector-specific use cases, and I assumed that meant the use case group would go back and dig up the sticky notes and make them something somebody other than the use case group could use, because I would argue they're not consumable right now, but there's a lot of really valuable information there. So we purposely, in the use case group, did a lot of detailed work and then ended up with, I'll call it, a very abstract document that we sort of did that on purpose, but now for Phase 2, we can afford to go to that next layer. We don't have to go down to the bottom of the pyramid, which is where the sticky notes are. We just need to go to the OK for health car, you do this; for automotive, you do this; for security industry, you do that. I assumed that was covered already, but if it isn't, I think it should be a specific point.

>> FRIEDMAN: Great. Thank you. And it's a good segue way to the next part, which is we start to get to the hard side of things of how are we going to get all of these things, from page three here -- because only two of them are about the things that sort of identified as Josh -- hard problems left, not to mention sort of the original set of suggestions. And we have a number of existing working groups. What I don't want to do is try to distract from getting Phase 1 done. And so what we can start to do is say, "What are the things that we want to prioritize, and what might fit into the existing structures that we have today, and when might it make sense to think about saying, "This working group is finished? We can stand down. this working group as an organizational structure and spin up a new."

We can have as many working groups as you like. I would not recommend having too many if for no other reason that it's good to have a decent amount of overlap or at least a little bit of overlap other than just having be the at the core of everything. But all the things that we've talked about today, are the things that folks want to prioritize, and from there, we can start to go into the what are the priorities that makes sense to cluster so that we can start -- that they're going to have similar style work, so that we can be efficient about doing it and efficient about sharing it out. Jim.

>> JIM: I just want to confirm that the assumption there is that the existing working groups have a mandate to continue.

>> FRIEDMAN: Yes. The existing work groups have many to do inasmuch as they would like to. But again, this is the joy of having a structure that is defined by the participants. We have path-dependency. We've got some good rhythms now. I've learned that I shouldn't plan on doing any work on Friday other than this. But I think, at the same time, what I don't want to do is hold us to some of the commitments that we've -- the structures that we have. So this is the tyranny of the freedom that has been placed in your hands, as you can define this however you like. Certainly basing on off what we have makes sense. The health care proof of concept group, I think is functioning very well.

A lot of work has been put into it. And so don't want to say you guys have to abandon and then reform out of whole cloth. But I want to put it on the table that if folks say, "You know what?" For example, I'm going to call out the formats group. They say, "We still want to talk about tooling, and maybe in the quick start guide," but from the tooling perspective, it makes sense to say, "Hey. We're going to focus on the tooling in this domain over here, and the folks that want to focus on tooling this domain can go over here." And we'll try to coordinate to make sure that everything is is easily presentable, so that folks can find it all. But we don't -- we want to be creative. There's a chance to sort of say, "What can help us get the work done that we want to get done?" Duncan?

>> DUNCAN: Okay. So, three points. First point is, if we could meet not on Fridays, I would certainly appreciate it. Now summer's over, it's not quite as bad, but Friday afternoon on a summer for a meeting it's just tough to make. But my actual real point's on things where I think focus could be assumed in that comment was that there's value in the healthcare POC continuing. I have nothing to do with it, but I really hope they continue it. That was great work and I hope they do a second version. So I'll vote for that one. Yeah.

>> JIM: Yeah. I think it's a realistic assumption there.

>> DUNCAN: Okay.

>> FRIEDMAN: Try to stop, Jim.

>> DUNCAN: Okay. And then my second one of where I would put priority, and again, people might not naturally see it, but I think there'll be more value there than you think, is in this high assurance use case. I think there's much more value there than just for special gov-y stuff. I think it will actually get into a lot of these other issues we were talking about. Thank you.

>> FRIEDMAN: Fantastic. Let's make sure that we spent some time talking about the high assurance model. Are there... Josh?

>> JOSH: I want to fuse that with the suggestion for a maturity model because we were talking last night as well about a maturity model but because it can be an implied roadmap, you know, the crawl walk run or the, because maybe I think we have mislabeled this, the DOD high assurance thing. I think there's just degrees of participation in quality and perhaps fused with the maturity model we may have the ability to map what you do next. No matter where you are. This is what you do next. Friendly amendment.

>> FRIEDMAN: Nope, I think that's great. And I think I'm very happy with the document as it stands because it's written the, that assurance appendix sort of lays out here is the value add of doing it right in SBOM as it currently exists is kind of in the, I think that the security term is keeping honest people honest. If you're interested in detecting active subversion in the supply chain, well, a hash will help and some of it won't help. Right.

An SBOM won't prevent someone capturing keys and doing it except you carry it to the logical conclusion, which is I've had conversations with people who say, Oh, the entire way we do developer keys is broken. So let's dive into the high assurance side of things because I think there is a risk of having it devolve to a reproducible build or nothing. And I'm sure a lot of you know folks in the security software security space, which strongly believe that. And that's very important for certain spaces. What else is there that we would want to try to think through from this appendix? This one. Duncan?

>> DUNCAN: I think it's more than just the appendix because we didn't include everything in the appendix but the infamous teapot picture, if everyone remembers, that has this sort of all the the lines going out with all the different verbs besides contains. Basically the current framework we're in. We're ending up with just basically Hey this software contains this other piece of software and we ended up with like, I don't know, seven or eight other verbs there. I think those aren't in the appendix but I do think they are fair game. I think we need to do them, that includes the removal part in a sense, it includes the issue we got before it's not complete unless you have all the sub pieces. But you made it by taking this complete thing that had eight sub pieces and taking out the one. There are ways to specify all

that. It's more than just the pedigree and providence and integrity. It's also the completeness of the pictures we were talking about before.

>> FRIEDMAN: And are there specifics, so for example, Lori talked about maybe implements is the right verb?

>> LORI: It's like, I'm not sure if it's the English word, abstractization.

>> FRIEDMAN: Abstractization, okay. Which is to say this is the implementation of that abstract.

>> LORI: And that if needed you can swap it out for the other one.

>> FRIEDMAN: Okay. Are there other things that you would want to put in that-

>> DUNCAN: Well, all the other ones are on their chart, there was inherits from, there was the real-time update one. There was like seven or eight of them.

>> FRIEDMAN: Okay. Art, I think that's one of your images, if memory serves.

>> DUNCAN: I think it was the teapot that had the inherits from it had the real time download of the software. It had all the different things you could put on the line between--

>> MANION: Sean didn't get blame or credit for the teapot I think. He's not here to defend himself. Definitely going to blame him.

>> DUNCAN: All, of those, that's all I'm saying.

>> MANION: The, point in phase one's relationship is includes with a note that you might want more refinement, but we're stopping short at this point of going into those refinements.

>> DUNCAN: But I'm saying as part of this high assurance thing, you need all those other verbs.

>> MANION: Probably, yeah.

>> FRIEDMAN: All right. So on the assurance side, integrity is something that I think we've started to capture in the framing document which is signing. As we all know cryptography is easy and key management is even easier and so we'd probably could benefit from having some discussions around that. On the assurance side, are there other things that people want to sort of throw in the assurance bucket at this point? Yep.

>> LORI: I am not sure if it completely fits in there but basically to sell the high insurance model, you would need also kind of like a negative views case study. So if you don't do that, bad things will happen to you.

>> FRIEDMAN: So we have some great work that's been published over the last three years by a CITL that's done a longitudinal study of consumer grade firmware in home routers and other devices and they've shown that there is no systematic progress in firmware protection. So, you know, non execute,

things like that. Thank you, ASLR, that it is not being used. And so is this the sort of thing now that, what I like about their approach is they've got a very small universe.

>> FRIEDMAN: They've said six attributes, they're stable, we're not inventing brand new things for this level of technology. And this level of technology isn't terribly complicated, but it's stuff that use available in most development kits today or most build kits today. Is that the sort of thing you'd like to sort of think about as part of the assurance approach?

>> JOSH: I think for this working group, we should look at the elements of an SBOM that could support integrity and high assurance, not the entirety of higher assurance. So I mean, I know you have to be literate on those abuse cases, but I don't want this to become an another accidental multi-stakeholder workshop.

>> FRIEDMAN: Good. So can I push back on you for that? Are there elements of the SBOM, because I agree with you completely. I think that if you're trying to capture all of development in your SBOM, you're going to have a whole lot of data structures that you need to think about, many of which aren't defined in the systematic way. Are there a couple of things that you want to flag?

>> JOSH: I mean, just to foot stomp what somebody said earlier, whether it's Art's crop circles or Chandon's, you know, flower petals or teacup or whatever the heck you guys want to call these things. I think we had some work that could be revisited in a subsequent phase, but I don't think the goal is to come up with every high assurance use case. It's really just to understand what's the body of work of high insurance use cases that and how would we support those. Just a scoping statement.

>> FRIEDMAN: Great. Thanks. All right. Other things that you'd like to prioritize? So we've talked, we've had some conversation about thinking about high assurance, thinking that from a use case perspective, powerful. Are there other things that we've talked about so far or that are on this list that you want to prioritize? Mike? Sorry.

>> BRUCE: The supplier name.

>> FRIEDMAN: Good. So having a discussion about naming?

>> BRUCE: Yeah. No, really getting it done. I mean, you know, getting it assigned to something.

>> FRIEDMAN: Okay. I think that's a good, that's something we can prioritize. It fits in with I think some of the existing workflows.

>> JOSH: Just to render what's a private conversation earlier, I'm trying to non rhetorically ask what's the best starting point because CPE for example with funding didn't do it. Do we start there? Is there an alternative that you have in mind? Like who logically would make such as a directory of these things?

>> BRUCE: Well there's, if we could persuade first to do it, that would be great. But as far as I know, they only do it for vendors that are members of first. If we need somebody else to do it, then we need to select somebody. CV to me would be a logical place.

>> ED: You mean CPE or-

>> BRUCE: The CVE organization, the organization that create that.

>> JOSH: You did say that you-

>> FRIEDMAN: Katie, just to start, there's a chalkboard, could you start writing?

>> KATE: Yes.

>> BRUCE: I don't think it can be a vendor. I mean, there's plenty of vendors that would do it. We would do it, but we don't. I don't think that would be appropriate.

>> FRIEDMAN: Are there any of the consortia that you're involved in like a KC? Would that be a good one or not?

>> BRUCE: I don't think [INDISCERNIBLE] would do that.

>> FRIEDMAN: Okay.

>> BRUCE: I think first is a better guess, but of the other ones, I know-

>> FRIEDMAN: If only we had someone involved in first.

>> MANION: Actually I'm going to say exploring first is a reasonable option, but I have my doubts that it will go there. I fully agree, this has to be addressed. It is my hope and very low confidence belief it can be done without a central authority. I do not think a central directory is going to fly, but I don't have an answer as to how to federate it like the other stuff. So anyway.

>> FRIEDMAN: And just a quick bit of history, I'm going to wear my Dave Walter Meyer hat here, there was in fact an attempt to centralize this with the common platform enumeration, part and parcel of CVE and CPE. The challenge was that the resources of that organization, they didn't see it was possible, you know, software ate the world and there was just too many things for them to enumerate in a centralized fashion. So it was good for having a format and a single place to look as a way of listing all suppliers. Aliasing may be something that could be a little more finite, especially when we start thinking about our supplier level.

They had an initial vision, but I don't think it sort of has emerged, which is just to say, Hey, have everyone do it themselves. And that's kind of what we're hoping for. So if there's some vision that we can sort of have for further guidance that doesn't say you have to do it our way, but just make sure that you have a way of doing it. We've got a bunch of two finger comments. I've got Mark, I've got Duncan, I've got Brenden, I've got, Oh my goodness, I forgot your name.

>> ED: Ed.

>> FRIEDMAN: Ed, thank you. Okay.

>> MARK: So I was just going to point out that just recently had the experience of how does Google solve this problem for when they, you know, are bringing on vendors and other things that they're working with and they use ICANN. And basically their solution is if you want to onboard to our system,

go get yourself a DNS because the one thing we know is that a DNS name is unique and verified to an address. And so I actually think that this is, this is the sort of solution we should be thinking about. You know, it actually makes a certain amount of sense.

>> FRIEDMAN: All right. Kate, do you want to two finger on the ball?

>> KATE: Yeah, just quickly. This is actually something that we've been working on with the licensing on SPDX and certain companies want to have their own namespace of licenses for their proprietary licenses and so there is a proposal for a namespaces using the DNS side of things there that might be a starting point to look at.

>> FRIEDMAN: Piggyback on that. Let's see. I'm sorry, the order, Duncan. On that exact point, two fingers.

>> DUNCAN: Yes. Well, on the exact point when I raised my hand, which was the point before. So if we could be clear and we don't have to solve it now, but when we do solve it, if we could be clear, if we're talking about the name of the software that goes in the SBOM at the time of vulnerability or, worded differently. Traditionally the names that have went in CVEs when CV got suggested is at the point of vulnerability, not at the point of creation of software. I think we're being clear now that we're trying to pick a name for the software at its time of creation so that every piece of software has one of these, not just once you've found the vulnerability is a question. And I'm not saying we have to solve it, but that confusion has confused us in the past. So we should make sure it doesn't confuse us now.

>> FRIEDMAN: I worry because this morning we talked about this exact problem, which is software names are not immutable. So I don't think... yeah. Brenden. Oh, Mike, sorry.

>> MIKE: So also going back to the point at which I raised my hand, I would put in a note, not just because it's convenient to us at Get Hub, but also because I think it's helpful. Instead of considering this as a Federation problem for naming, just consider it as a name spacing problem. So in our dependency graphs, we often have, you know, here's your Get Hub name, which we know because it's on Get Hub and you publicly published it, then you may have a separate say NPM name. But we know that. And so we can just give your name either the vendor name or the software name, it's often different in all four, like all four parts of the Punnet square to say this software is named this on Get hub, it is named this on NPM. And just give it a prefixed name as we track it through our dependency tree. And that way we don't need to have a central authority. We can have a bunch of kind of well-recognized namespaces. And if you don't recognize where it is, go find it on DNS or whatever.

>> FRIEDMAN: Ed and then Bruce.

>> ED: Yeah, just kind of, you know, to me part of the challenge is your first defining what is it we want within our SBOM world. So what makes the most sense as far as, you know, establishing clearly and understanding the identity of these components and the items that are being described by an SBOM. Because I think once you understand that and then what needs to be put in the SBOM, I think that'll help you figure out now how can I use that as I interact with other systems. So really I think it needs to be focused in, you know, in these groups first before we, before we go outside.

>> FRIEDMAN: Okay. No, I think that makes sense. And a generation and then mapping. Bruce.

>> BRUCE: Many products have multiple names simultaneously, particularly different versions of the same product where the fix has to get back ported will have different names for the different versions. So we can't, so the question about whether that's the version when reported or when the software is made, it just has to be handled with aliases. We can't distinguish there. You know, the other issue is a DNS names, and this is a detail, DNS names sound like a good idea but huge numbers of people can't get a DNS name. So another approach has to be taken. In the third party components where I work, which is like 3000 I think something like over 1500 are names of single individuals that are the supplier and most of these guys don't have and ladies don't have those, you know, a DNS name.

>> BRUCE: So you know if if you want to get Get Hub, which is what, Microsoft now? As a place to store the name, you know, some people might object to that because it's Microsoft that's been objected for other reasons. So you know, the thing is what I was trying to say before is we need to get a solution here somehow that's acceptable.

>> FRIEDMAN: We don't need one solution. That's the point.

>> BRUCE: If you want to communicate between multiple people, you have to get, you have to know where the solution is that you need to figure out, who the vendor is at least or the supplier is for the software. And if everybody gets to make up their own, it's going to be very difficult for us to figure that out. Maybe you can run Google or something to find out all the sites in the world that have the name Cybil in it or whatever name you're using that's looking for it, but you know, I don't think that's really feasible.

>> DUNCAN: Okay. So besides when we get around to solving this, dealing with the time aspect, at what point you make it, I think to Bruce's point on the aliases, just because historically people have used lots of different names for the same thing, does not make it a good practice. I think we have to discuss what is where we want to get to and if where we want to get to is have 10 names for the same thing cause it's best for the following reasons, that's great. But if where we want to get to, if life would be more secure, if we only had one name, we at least could give that as where we'd like to get to. And what would it take to do it? I don't think we should get too tied up in solving. Yes, we have a lot of old problems we have to solve, but we should still also try and look at where would we like to be.

>> FRIEDMAN: Best practices for naming, we'll add that to the list. Mark and then I think we'll...

>> MARK: I just wanted to say I, when I suggested ICANN, I was specifically suggesting ICANN as the source for name spacing names, not that each individual supplier by the definition of an individual coder would be, you know, going out and getting a DNS name. But you know, if we wanted to, you know, in a federated model we have to somehow identify the unique suppliers in the Federation and DNS seems very appropriate because let's be honest, in most cases, we're talking about things that probably already have DNS names that are going to be those things.

>> MARK: And maybe Get Hub users is kind of a top level domain for that and then Get Hub is that top level domain or Maven central is a top level domain or NPMJS or whatever. You know, I think that's, when I said ICANN, that was what I was talking about, not for the individual component.

>> FRIEDMAN: Thank you. Just a reminder for folks on the phone, if you want to weigh in on this, star one. If you're having some issues, try to back channel. Melinda, I don't see anyone in the queue. Is that right?

>> MELINDA: Thank you. At this time, there are no questions in the queue.

>> FRIEDMAN: Thanks.

>> FRIEDMAN: Always good to make sure that your data system actually correlates with reality. All right, Josh, do you want to close this out on naming?

>> JOSH: Yeah, I just want to synthesize because there's lots of good stuff, but some of them are talking past each other. Duncan is 100% correct that if we're going to create an SBOM at the time of creation, which lots of our other bodies of work says we should, whatever name we pick can and will change later. So therefore, using Art's prior document that the SBOM MVI does not include vulnerability stuff but it can reference a different resource that has vulnerability stuff, SBOM's going to have a name supplied that may change over time, and should, the second resource needs to exist which is a list of aliases for that thing. So, I'm kind of repeating what other people said, but the temporal nature is when you create the software it's going to have an name which cannot be guaranteed to stay the same forever and therefore, it necessitates an alias directory somewhere. And no you don't have to use blockchain... Meantime to blockchain six hours.

>> FRIEDMAN: All right, so I want to start getting into how we're going to tackle this but before; I want to allow folks to try to say, this is, you know, one last thing you want to try to put on the priority queue. Is there anything else that someone wants to emphasize? By the way this doesn't lock anyone in. The work that's done will be done by the people who are doing the work. And as you remember from how this process began, things evolve over time. They'll merge, they'll separate, we'll get false starts. That's okay, right? That's the benefit of agile policymaking. But if there's something else that folks liked that we've talked about today or that are from this list, now's the time to try to flag it.

>> FRIEDMAN: All right, well let's dive into what's actually going to happen next. What are we going to do? Cause I think this is really inspiring. Humbling, right? Still a lot of work to do, but I think it's time to sort of dive into this. So do the buckets... They're still right there, there are some things that cut across a number of the buckets. But in terms of the work to be done, one Healthcare POC, you guys I think are happy moving forward, give me a second, happy moving forward. You want to extend it, you'll want to sort of engage in the broader community but as an organizational factor, you're happy with this? Yep. Okay. Thumbs up, Duncan!

>> DUNCAN: So on the Healthcare POC we have both a reasonably closed group with very specific focus, and a broad term objective in phase two to involve other sectors. That seems contradictory to me at the moment. So the Healthcare POC is going to continue as a Healthcare POC.

>> FRIEDMAN: Yeah.

>> DUNCAN: That will naturally stay a Healthcare POC unless we do something different. If we want to get--

>> FRIEDMAN: Their report clearly documents the fact that they're going to reach out with a bunch of vendors at various levels of the work.

>> DUNCAN: No, I meant to other sectors if we want to get a sector other than health care involved in...

>> FRIEDMAN: In the same Proof of Concept?

>> DUNCAN: Well you have a bullet

>> FRIEDMAN: Yup.

>> DUNCAN: that says extend it to other sectors. If the default is we're going to have two separate POC's, that's a different issue. If we're going to have a POC involving multiple sectors, it has to be more than the Healthcare POC is all I'm saying.

>> FRIEDMAN: Sorry for the clarification, I think if folks want to jump in,

[CROSS-TALK]

>> FRIEDMAN: -- follow on to healthcare Proof of Concept and then other sectors present a Proof Concept.

>> DUNCAN: And my reason for.

>> FRIEDMAN: Proof of Concept.

>> DUNCAN: Well my reason for bringing it up is because of the policy and legal issues which were clearly non-trivial in the healthcare industry. It was more closed than it would naturally be. Say somebody from automotive wants to just join it and make it an automotive, that isn't going to happen unless somebody does something.

>> FRIEDMAN: Let me try it again. Proof of Concept we need the institutions first; and I know that a number of you in the room and I are actively working on that now, but it starts with the people who are going to be participating and then from there we'll see what we can do. I thought that both Jim and Michael [inaudible] actually did a phenomenal job of making it a very open process. Despite it being an NDA'd actual sharing. They did a really good job of making sure that everyone involved who was not a direct participant knew exactly what was going on as it was going on, and could even weigh in on a lot of the details...

[CROSS-TALK]

>> DUNCAN: Which I applaud them on, cause I'm not a healthcare person and I got to do that. So yes, they did that very well. I just want to make sure it can get extended, that's all.

>> FRIEDMAN: Thank you. Lori?

>> LORI: Would it be possible to get some kind of overview of a process to doing a POC?

>> FRIEDMAN: Yes, I think there's...

>> JIM: Yeah in our previous documents our process is described.

>> LORI: Thank you.

>> JIM: In fact in the report, the process is described as well.

>> LORI: Thank you.

>> FRIEDMAN: Yeah, just the brief overview of one of things that again worked really well is a priori defined use cases was perhaps one of the most important components of that, so that they were giving themselves an actual scientific challenge. The documents are great they sort of went through here are the decisions we made, we decided to do this, we decided not to do that. Les?

>> JIM: Go ahead. No, go ahead.

>> LES: To your comment is there a desire or an objective to standardize some type of SBOM across industries or was it just to involve them so they do one...?

>> DUNCAN: One of the objectives when we first started this whole mass was the FDA came out and said, "Hey medical device manufacturers, you've got to do this." And then it looked like it was at least possible that 17 other government agencies were going to do the exact same thing in an industry. We're going to end up with 17 different sets of rules to follow. So NTIA said, whoa that's probably not going to be the best in the long run. Let's see if we can get one set of rules to follow, and if this FDA set a rules; if it was used by the DOD, if it was used by I don't know, Social Security Administration, whatever other ones needed it, we could come up with one way to do it that would benefit everyone." And I think we've all in our heads reached that conclusion, and we even had that as sort of an objective to try and reach on the POC. But with only one you can't do that; so the hope would, or at least my hope would be we could sort of prove to the world there's actual value to PTC and that it to device manufacturer one it did this, and the auto manufacturer two it did the same thing, and look there's value to that. So that would be my hope, it might be an unrealistic hope. But I thought that was the whole reason for the multi-sector.

>> LES: When we started this in, and my recollection is, you are correct, right? What happened with us, myself, and in this area was we said, well to do this we've never done this before we want a Proof of Concept. So we just went after that right? So then we did our Proof of Concept. So I don't disagree with you. We would like for other sectors to come into that, now should they be in part of this Proof of Concept, we can all debate that right?

>> FRIEDMAN: I feel like we're now talking in circles. I think by definition executing a industry specific, an organization specific, thing is going to be a bespoke process. Anyone who moves forward, hopefully will have this great path to follow, and if we can involve multiple sectors that's lovely. The whole goal is to get more organizations doing this, and that I think, speaks to documenting successes. It turns back to how are we going to do some of the stuff we've talked about. So yes, Jim,

>> JIM: Let me just bridge to that. What we said in our conclusion was that what we came up with; the approach, the processes, the formats that we used, it is directly applicable to other sectors, other verticals, right?

>> FRIEDMAN: Completely.

>> JIM: But, the proof of concept itself was because there was a nexus of people in both the consumer side and the production side who were willing to do that.

>> FRIEDMAN: And I will go one further just to to put a point on the table. Something that this community was very clear to do last year was to define, this was last fall, define what they were doing not as a pilot but as a proof of concept. Now something that we can start to think about putting on the table is if we now know enough to know that we're going to be heading off in this direction, do we want to be considering the pilot? But, I want to leave aside the POC model because again; the folks in the healthcare space I think have their legs under them, and have in the course of doing their work sort of have thought about what they might be next, or at least thought about how to think about what might be next.

>> FRIEDMAN: So the next question is; when we think about refining this model, documenting further successes, strategies for awareness and adoption, and tooling, sorry tooling processes and services, thank you, what are the mechanisms that we're actually going to start working on this? Because again, it will take some time for us to self organize a little better. Where do we want to start with this? And so, one option is just to go to the individual working groups and say, hey all of the things that we've laid out, does it make sense to stay intact? Or do you want to sort of say, hey our mission is done for our short run and we're going to sort of step back and then all of us are going to step forward in slightly different re-organizational structures. So I think there's value to think about both sides, Josh.

>> JOSH: The way my brain works is I kind of needed to see this whole thing and kind of affinitize it. My hypothesis is some of these will naturally fit with the existing momentum and groups that we have. Some of them are unlikely to happen with the existing groups we have and we probably want to spin up adjacent ones. For example, with the coordinating vulnerability disclosure one we did, there were some surveys and some PR and marketing personnel that understand the finer points of communication, we haven't attracted a lot of those folks. We have some by accident, we haven't deliberately done so. So I'd want to like cluster these maybe after I've looked at the whole document, maybe not work shopped right now, and at least propose; we think there's a natural fit to have the use cases ones do this, but we don't see anybody yet that's a natural fit for this. Could we spin up another group? So not an answer, but a step towards an answer.

>> FRIEDMAN: Thank you, and I like what you're doing because I think we can have a straw man approach to it. So for example, Art just stepped out of the room so we can start with him, right? The folks who've been thinking about, let's whiteboard out what this looks like. Well I know that Art's group has already had a discussion of naming. I know that they've had an initial discussion around what transparency looks like in some of these sort of further refinements of defining this stuff. Could be a decent fit, on the other hand, folks can say no it's not. Similarly on the use case side of things, doing a renewed push to find the demonstrated successes, having the stories to tell, there's a lot of that that directly feeds to witness and adoption. But it also is in very much the the demonstration side of things as well as tooling needs and high assurance needs.

>> JOSH: So on that front, we have a couple people from GIT or from JFrog or some of the tooling, but I believe we might attract more folks from the tooling if we had an ambassador initiative for the development ecosystems and languages. So that maybe that fits in an existing one or maybe you need to build it and then they'll come.

>> FRIEDMAN: So let's, let's talk about tooling.

Speaker 8: So, going to building on the recurring cycle and discussion of this morning. My thought was that tooling and standards and formats go together pretty well. Because I think as we build more tooling, I've been sketching tooling and unfortunately it's not in the state I can share with anybody, I've been noticing, Hmm this doesn't quite fit the way I need it to when I go from two or three dependencies to five or 600, thanks Node.js. So I think enabling that dialogue to continue so that we can frankly rewrite the formatting as we discover major problems. Would be helpful.

>> FRIEDMAN: Great. I think a something that Tate has talked about is saying, you know, as we begin to think about slices of tooling, there's a natural way of thinking through things. So for example, what are all of the tools that we have today that can generate a SWID file from a build process? What are all of the ways that we have of... Kate do you have some further examples?

>> KATE: Yeah, how do we go about analyzing into Container and the implications of using a container in the remote services. How do we basically deal with things that are updatable in the fields or not updatable in the fields. There's a large space that I think we could probably start looking at saying, okay we want to handle this type of scenario, what tool is there? What's not there? What do we want? So lots of scope and yes, I agree it'll form, here's some gaps in our formats and it will also form how do we get to the next step. But doing a survey here seems like it's a useful exercise.

>> FRIEDMAN: And so let's continue to pull this thread of the folks that are going to be thinking, because I think it makes sense that the formats group started off as the folks that were committed to saying how do we build this stuff and so it's a natural segue into it. Identifying needs that aren't met today is going to be a big part of that. There's going to be some work that the use case group is going to probably want to find some way of engaging in, but I think it makes sense to sort of have the operational collection happen at the S&F group. Duncan.

>> DUNCAN: so I agree with tooling goes to format that one makes sense to me. The sentence before you said that was that the use case group would do the new use cases for all this other stuff we're doing, and they do the awareness and adoption. From my view, there's a gap in awareness and adoption, in other words, there's an awareness and adoption issue independent of the other three groups. I do not think the use case group should accept all of them.

>> FRIEDMAN: Agreed completely, right it's on here in that framing because it's a set of needs that are cross cutting, and just as champions in the sectors, maybe a use case group expertise has sort of built itself around that? You know, we've got automotive, we've got financial, we've got DOD land, but of course on the technical community that's probably a different approach. Are we ready to start thinking about a higher level strategy for awareness and adoption?

>> JOSH: I do see it as a matrix I guess to put it slightly differently, because if our group's R&D and we've captured a bunch of products for these different sectors, we still need a marketing team. And so with the developer marketing from standards group, so an abstracted marketing team, I wouldn't call it marketing, but it does seem like,

>> KATE: Outreach.

>> JOSH: we could each use more outreach, inbound and outbound.

>> KATE: I think it's sort of relates to the comment about having a gold deck so that we all sort of roughly stay on message.

>> FRIEDMAN: Yeah, We are all in our own worlds and, right? A lot of us are in the business world. We're competing. That's great. And so I liked the term of you know, have a common message as you go and talk about these various things to do, sell widgets, or do what it is that we're doing. So I think that's a great point. Cait, putting on the spot for that one. Is that something that you think we may want to stand up a new group from folks that perhaps have a little less in the weekly meeting and a little more commitment to do an active mailing list type engagement. Is that something that would be useful?

>> KATE: That would work? I'd say try it and if it isn't working switch to another method, but I think having something that's common that everyone can go and see and comment on, it's been working well for the documents.

>> FRIEDMAN: Yeah I think I agree. Duncan.

>> DUNCAN: Starting out like I'd hope we'd want to end. For any new development of documentationey stuff which I would consider the awareness and adoption stuff to be of that category, we want to sort of come up with the common decks and everything. I would recommend to try and do it in something like GitHub doesn't have to be GitHub, pick a different one, pick BitBucket I don't care, but software industry has put a really lot of work into how to do collaborative work offline. We don't tend to use it, other than we use, you know, Google docs and I don't think that's the best way for developing this message stuff, particularly cause I'd like the idea of issues, I like the idea of seeing who made what change and stuff. I'd rather start there.

>> FRIEDMAN: So, I'll give you just sort of a very brief NTIA perspective, which is if you're writing an academic paper, you always want to do it in lock tech with bib tech, collaborating with someone outside the academic environment, you're going to have a bad time. This process is, usually NTIA processes, well the reason I really like them is because they bring together tech people and policy people. Having had to hold people's hands as they work through, introduction to GitHub, it's not impossible, just a little difficult. On the other hand, we're lucky, I think this particular community does have more technical people, or at least people who are familiar with GitHub and who have used it before.

>> DUNCAN: I mean, there's WYSIWYG, markdown editors and stuff. It's not as hard nowadays as it used to be. I don't know if you've tried using it all lately, but I'm thinking webpage stuff. I'm not talking about developing software. We're talking about developing web pages in a common spot.

>> FRIEDMAN: Any further thoughts? I think at a certain point it's going to make sense for a working group after they've defined a new scope to sort of have the, how we're going to, talk. I think that's a local decision that makes sense. But any further thoughts on sort of the modality of collaboration?

>> JOSH: I'm just going to be a little less diplomatic. I hate the idea of doing GitHub and it's not that's it's not good for a lot of the folks in this room. It's that there are so many other stakeholders where that is a debilitating barrier to entry, no matter how easy you make it. There's going to be management folks, there's going to be... I just think we need, I hate to say lowest common denominator, but there's a whole bunch of people I need in the fold that would never get in the fold if they have to a GitHub account.

>> DUNCAN: So just to be clear, I'm not asking it because you want them to be part of the development team of making these documents, I'm talking about for how we display these documents. A webpage you go to, you give them a link to get to it. How did we make that webpage? We're making the webpage. We're not asking them to make the webpage. If we're going to be developing that kind of documentation, and I would think we'd want this to be a link on the web-

>> FRIEDMAN: Kate, last word and then we'll...

>> KATE: I think we give mixed modes here that we can use. We can use things like Google docs for very collaborative ad hoc and then once we're all comfortable, we can log it up on something like GitHub so that it's more accessible and there's a history, but I think we're going to need to work with both.

>> FRIEDMAN: Yes, use the right tool, if your goal is to have a very solid first draft and then allow lots of people to edit it so it changes over time. It helps great. If your goal is to have an enduring static draft, PDF probably captures most of what you need. Okay, so we've talked about some of these issues about how we're going to get things done. What I'd like to do is start to get everyone to think about what's going to happen after we've all had a week or two to relax after these initial phase one drafts are done. So, and again, some things I think slotted up reasonably well.

>> FRIEDMAN: We've got healthcare POC. Ideally we'll have maybe some other folks by then who might be interested. We're going to be giving a lot of talks over the next few weeks and having a lot of meetings, try to bring more people into this room. On the tooling side of things, I think taking that punctuation and coming up with sort of a new set of charters, here are the things that we want to do. Not committing, but saying this is what we think our initial goals and work plan is going to be and then moving forward on that. So that leaves the used case group and the framing group. Used case group really had a tough problem, right? It was trying to get people to be honest about the work that they were doing and then finding a way to take that narrative and help communicate it to a broader audience. Thought that was a phenomenal job. Moving forward, is this a community that wants to sort of stay together and try to have the next steps? Josh, I'm going to put you on the spot for this one. You can say, yes it's a great fit or you can say no, it is completely fair to say the work that we have to do doesn't fit perfectly with how we were organized and so we can disband and then re-come together.

>> JOSH: I'm chewing on this. I think Duncan might've helped me a little bit. I just drew a little three-level pyramid where we started at the bottom with ground truth and I don't think this group was ready for that yet. I think we will become more ready for it, but then said it wasn't consumable and I think our dockets... So, at the bottom of the pyramid, which is a fact based of way too much detail, we have a good start, perhaps it can be packaged better. Top of the pyramid is the doc that we are circulating for review. I think what we're looking for is the middle tier, which is maybe a one pager, consistent, really readable and consumable. Abstraction of those sticky notes things.

>> JOSH: So my hunch is we can absorb it, is the short answer. The part I'm not sure we could absorb and I do think we need some extra help that's not in the room, because we've repelled them or failed to attract them is, who's going to come up with the strategic agenda of, these are the developer conferences we should have an S bomb talk at, these are the regions we should go to, here's the canonical. I just use the word canonical. Here's the most effective set of slides to pluck from, here's blog posts or podcast we should be on. The outreach part is a different skill set that I think we have in the room, with apologies to anyone that is in the room, but most of the talkers have a different skill set and I think we have to augment it with that latter skillset.

>> FRIEDMAN: I want to be clear that one of the things we'll be doing as we move to phase two is really pounding on people's doors and say, Hey, there's a lot of new work to come and get involved in. Come join. The question that I want to try to at least get people thinking about now is pulling on your thread here is, Hey, there's the capturing experience and then there's this awareness and adoption piece or outreach. I think you did a great, that's even better than awareness and adoption. Is that something that still could be under those auspices or should that be a new group? And if other folks have a chance to chime in, I think something that Kate hinted at is that could be something that would be a separate working group that didn't necessarily have to have the regular weekly phone calls because they weren't going to be drafting a document after they came up with a high level strategy. It would be, let's have regular check-ins. Let's make sure that we have situational awareness through other tools.

>> JOSH: I guess at the moment, in lieu of another home, we can be the default home, but I do want to attract people like a Jenn Ellis or others that could maybe organizing cross-pollinate.

>> FRIEDMAN: If anyone is fond of swearing heavily with a British accent, we need you.

>> BRENDEN: So I'm not necessarily the right person to lead the outreach efforts, but GitHub does occasionally talk to some developers who don't think we're just Microsoft and we're happy to do things like publish on our big blog and generally all the outreach efforts we have, it's a little late for Universe, which is our. Megacon, but certainly come next year, there are ways we could integrate into satellite, which is our European conference or a year from now. We have some resources we can throw at evangelization.

>> FRIEDMAN: I want to fork that conversation because I see Kate jumping at this.

>> KATE: There's a lot of events that go on at the LF and I keep a track of a lot of other related ones that I'm happy to pull into a master sort of set that are developer related and certainly happy to crowdsource a master set to go after.

>> FRIEDMAN: So let's spend five minutes now, not enumerating every single developer conference, but enumerating classes of types of events or communities that we would want to engage or could think about engaging. So we've got developer conferences and can we subdivide developer conferences by language or universe by tool. How else do we want to subdivide developer conferences or developer?

>> KATE: I'd also say we want to reach out to the legal community.

>> FRIEDMAN: The legal community, all right. [inaudible 00:07:58].

>> KATE: And the supply chain community, as well as the security.

>> FRIEDMAN: Hang on, I want to tease those each. When you say the legal community. I've even met a few lawyers in Washington DC. Are there other-

>> KATE: So I'm thinking like this compliance, [crosstalk 00:08:18] and export control. Not just licensing, but there's people who care about what is actually going through people's hands that have a perspective here to be bringing to the table.

>> FRIEDMAN: I have a good relationship with the folks in the offices on the floor directly below me, office by the name of DIS, so they handle that in government. So you'd mentioned that and you said supply chain. Can you be more specific on that?

>> KATE: So there's various conferences and areas I'm not comfortable with knowing about with supply chain. I was talking to someone who was working on brokerages of things going through important export boundaries and things like that. That part of it, in particular, I think there's pieces that they're going to want to interact with and they're going to be wanting participate in eventually, and so reaching out to some of the more traditional supply chains, the automotive supply chain, for instance, things like that.

>> FRIEDMAN: Excellent. Thank you. And I know that Bob has been running for, what, 15 years now? SSCA the supply chain-

>> MALE SPEAKER: [inaudible]

>> FRIEDMAN: Oh wow. I didn't know they'd been multiplying how productive. Duncan, classes of outreach.

>> MALE SPEAKER: Oh, [inaudible] Josh is right on point. [inaudible]

>> DUNCAN: Sorry. So three points. When I raised my hand with a two. You have now gotten into solving the issue as opposed to the original question of, should it be one of the existing groups or new working groups? So I guess I would vote for new working group because, as Josh mentioned, there's a class of people not here, the people in communication.

>> FRIEDMAN: And we talked about that, yes.

>> DUNCAN: I still vote for that. But now on your particular ones you're asking for, I think you need to go at a class of people called the executives. So things like CISQ with the trustworthy manifesto. I don't know if you've hit them up but, they actually have in there, you got to have an S bomb is in the trustworthy manifesto. So, hitting up like them and to the legal issue, I don't know if you've hit the legal hackers group here in DC yet, but you should give the talk at legal hackers.

>> FRIEDMAN: I've had several interns who went on to run that community. So the legal hacker side of things... So let's do Jim and then Josh.

>> JIM: So those are what I would call horizontal communities. We should consider vertical communities. So I mean the obvious one to me is health care and medical device.

>> FRIEDMAN: If only we already had substantial penetration in that particular vertical, of all the verticals and the entire digital ecosystem. Let me turn that back to you. I joke a little bit but that's one that I feel pretty comfortable and I know that the sector coordinating council is keeping an eye on us and I know that the ISAC is watching us. Are there parts of that community that you think there's still a lot more work to be done in outreach, awareness, adoption?

>> JIM: Yes.

>> FRIEDMAN: A single word answer is okay.

>> JOSH: Excellent. So similar to that, and Alan just mentioned it, so this is less to Alan and more to the rest of us. In our most recent document, we do talk in that network effect section about the role that ISACs and ISOWs and sector coordinating councils can play, I believe you're talking to a bunch of ISACs-

>> FRIEDMAN: We are speaking to the council ISACs next week.

>> JOSH: ... So through that, each of those sectors may tell us what the right watering holes are for those verticals. So the energy folks, the manufacturing folks. So they'll just like we've done a better job on healthcare. There are other designated critical infrastructure sectors or even commercial sectors that could give us a roadmap. So the roadmap is go around and ask them for the roadmap of the the most strategic watering holes so we don't spend a lot of time on the wrong stuff. But if we're going to bring these topics to those, I too was thinking vertical.

>> KATE: Just going back to the overarching ones, safety is also another community we need to be reaching out to cause they have a distinct need for it.

>> FRIEDMAN: Safety?

>> KATE: Safety, critical, critical infrastructure.

>> FRIEDMAN: ICS. Yes. So we've had a number of conversations with particular vendors. I've been talking to the organizer of one of the bigger ICS security conferences. Are there other classes of, there's the ICS, GWG. Are there other sort of ways that we can reach into the ICS community?

>> JOSH: I know the one you were referring to you and that's kind of like the cybersecurity conference, but I think beyond that, there's industrial IOT, huge conferences that have no security content, but we could potentially bring some security.

>> KATE: Exactly. And they need the prominent stuff, too.

>> JOSH: One's even run by Josh's company. But yeah, I actually don't even mean that one. But yeah.

>> DUNCAN: So on your safety question, I don't know if ARC is one of the ones you have on there already. It's a big industrial one down in Florida. Once a year, my wife gave safety talks at it for ExxonMobil, that's the only reason I know it exists, but they care a lot about supply chain and they care a lot about safety and they know zero about cybersecurity.

>> MALE SPEAKER: What about Charlie in auto ISAC. Charlie was [inaudible 00:13:45].

>> FRIEDMAN: The auto sector I think is a great place to engage, and I'll be speaking at the auto ISAC summit in October. Are there other automotive venues or angles that we want to think about from engaging in that sector?

>> DUNCAN: Automotive one.

>> FRIEDMAN: Automotive.

>> DUNCAN: So scope question first. Do you want it international or you just want to stick US?

>> FRIEDMAN: We definitely wanted, and once we were done with this, my next question was, Hey, there are all American.

>> DUNCAN: So for auto, I just got back from Geneva from the Citigroup 17 meetings, which has a joint meeting as part of the ITU runs this consortia of standards groups involved in the automotive industry that has some acronym like ICE or something like that. I don't remember exactly but I can look it up for you, but that's when you might want to get on their agenda cause you can really-

>> FRIEDMAN: What's the first number after ITU for that one?

>> DUNCAN: Well, say group 17 was the cybersecurity, ITUT study group 17 was what I was at but they're just one of all the people who sat at the table and this group whose name I forget the chair of it, who was I think from high indy, but I don't remember, was at it, and it's got ISO, it's got ITU, it's got IEC, it's got the auto ISAC was there. It's got a bunch of them so I don't know when the next meet but you might want to be on that one.

>> FRIEDMAN: I will follow up with you about that. Other ways that we want to think about outreach?

>> MALE SPEAKER: Auditors? ISO auditors, audit community.

>> FRIEDMAN: ISO auditors. I know that the the International Accountants Association or whatever those letters rearrange, has done a lot of work in cybersecurity. This could be a new way for them to do it. I think that'd be the auditing community. I know we have a number of folks from the big three on our list. [Melinda 00:15:44] is anyone waiting in the queue?

>> WOMAN ON PHN: Thank you. We do have two standing by. Our first is from Joe, you're line is open.

>> JOE: Hi I'm Joe Jarzombek with Synopsys. I've been quiet on this whole thing, but you've been asking the question about supply chain and there's actually groups within the department of commerce who are running supply chain groups such as the folks at the NCCO. They're running a supply chain assurance industry day. It looks like the way they're coming up, based on the industry participants, as the solution for supply chain risk management for them is, by from the OEMs and you'll be good. That's how they're pushing it. They don't want to be revealing of what's actually inside their activities. I will tell you that's also true of the DHS sys I run-

>> FRIEDMAN: And Joe, I'm going to cut you off because I make a point to not have any negative discussion of other federal efforts at these discussions, but I think there is a lot of room to talk, especially because those efforts predate this, and so in some ways if they were running around saying S bomb is the answer last year we would have said no, it's still premature. Those are great things to dive into and I've spoken to a the DHS team, I'll reach out to my NIST colleagues and talk to them.

>> JOE: Okay, well with the ICT scrim task force, even in working group three, that's about information sharing. When I brought up the need for having S bomb, if you really want transparency to be able to understand that. And you will have companies who will say, absolutely not, I am not going to reveal my intellectual property.

>> FRIEDMAN: I've had a lot of conversations with our colleagues over at DHS. I, in fact, have asked them to to steer clear of the S bomb issue just because you guys don't want to have to start going to two sets of government meetings. So we try to at least have a little bit of effort on that from a lane perspective.

>> JOE: I'd like them to at least point to the efforts that NTIA is leading with the multi-stakeholder activities.

>> FRIEDMAN: Excellent.

>> JOE: That should at least be part of that. So we've had those conversations. Just understand that you've got other activities that are talking about supply chain risk management who want to steer away from S bomb.

>> FRIEDMAN: Thanks. That gets to a lot of the outreach effort that we're going to need. Next we've got Cassie on the phone who hopefully can give us some insight into the ICS side of things.

>> CASSIE: People have already mentioned all of this. This is Cassie Crossley from Schneider Electric. So once we get a comprehensive list together, I can definitely send it across globally to our standardization and organization that deals, not just with cybersecurity but with all sorts of different organizations to see if they have some thoughts and suggestions for conferences. And I agree with the whole, let's do a separate working group. I think that's the best way to approach this because this is a very large topic.

>> FRIEDMAN: Excellent. Thank you. I really appreciate it. So we have just a few minutes left. Josh.

>> JOSH: Just one more class without getting into the specific ones, I'd been starting to talk to insurers who care about this because this becomes a way for them to assess relative risk, so wouldn't know which conferences but that's a stakeholder group we could look at. That's it.

>> FRIEDMAN: Great point. Thank you. So a couple of things. One, I still want to talk to the framing group and see if we think that that is a good starting point to think through some of the refining and extending. And it could be that that group says actually it's not, but what I'm going to propose, as your straw man, is to say that group can be where some of those discussions start and we do a little more enumeration and prioritization. And then, if it turns out that simply the folks in that group aren't interested or they need further expertise or they say, nope, we're tired of doing this, we want to go become painters in Southern France, they can make that decision. Any thoughts and reactions to that? It's end of the day where people are just ran down.

>> LES: Art's thinking really hard, he doesn't want to answer, I don't think so.

>> FRIEDMAN: I think Art would look great in a beret.

>> LES: So when you say expertise, what expertise are you thinking?

>> FRIEDMAN: That's a great question. So as we start to think through some these issues, I think they're each going to have to have their own approach for expertise. So for example, a high assurance stuff, we're going to need some people who think about offense. You're building against threats. And so that

discussion shouldn't happen without having folks who have a very real understanding of the real time threats. Sharing S bomb data, operational considerations on the customer side as well as the supplier side. And by the way, that's a multi hop issue. So sharing from one open source project down to the next. It's going to look very different than how do I get my data to someone who's got an embedded device in a power plant. So having those different perspectives and of course commute the exploitability in context issue. That's heavy on the software engineering, software security side.

>> FRIEDMAN: So all of these efforts, just as the work that the framing group did it in the first place required many different perspectives to actually flesh it out. But that's I think one of the reasons it took a while is because we had to have all of those perspectives at the table to have the vision that the team wrote, that Art and Michelle wrote. I think it's going to further require that. Does that make sense?

>> LES: So you're wanting the framing group to comment on whether they want to pick any of that up? I guess I wasn't following exactly there.

>> FRIEDMAN: That, I think, would be the general vision is at least from the first wave now. Art, you wanted to [inaudible].

>> MARION: Yes. Just a that makes general sense to me. I would want to take this to the group and kind of gather opinion and consensus, but again... I don't know how many pages were on here of notes, but there's a handful of things here that probably fit in framing. My suspicion is the framing group in some form probably should continue, but decline to answer or make a commitment on the spot here until a little bit later.

>> FRIEDMAN: One thing that we always try to do at these meetings is we're going to post the video of this as soon as possible. It'll take a few days, but we always post the notes without editing because they're taken in front of you, for this discussion because it is trying to set up the next set of approaches. What I'm going to do is try to do a little more refining of this discussion and propose some tentative buckets as well as try to flag what I heard in the room today about priorities and so it'll take a little longer than usual to get the notes out from this. What I can tell you is that since we're starting this process in sort of a new direction, ordinarily I would say the next meeting be a virtual meeting. I try whenever possible to make sure that people don't have to get on planes. I'm aware of how unpleasant it is. I think that because the next meeting that we're going to have is really going to require some hands on discussion and refinement and the chance of different groups to start to talk across each other. I think it makes sense to have that meeting in person.

>> FRIEDMAN: The tentative date I have is November 18th or 16th? 16th thank you. Which is a Monday. It's not right before Thanksgiving. I looked and I didn't see massive conferences in either security, energy, or healthcare. Didn't look at the development world-

>> DUNCAN: Did you mean the 18?

New Speaker: [cross-talk]

>> FRIEDMAN: So then that would be the 18th, thank you. I appreciate you clarifying. We try to do our due diligence before we send it, put everything in writing. So the vision would be to reconvene here. Having had the first wave of potential discussions in the working groups, what we'll do beforehand is work very hard to communicate with the broader list. Most of you are in the working groups, you know

that those aren't massive work groups. There's a dozen each or so, maybe two dozen. Lots of lurkers and that's okay. Lurkers are important because they complain when something goes wrong. We've had a lot of stakeholders who show up just to make sure that we're not doing something that's absolutely terrible. That's great. That's how this works, but what we want to do is make sure that we can really reach out to the broader community again and hopefully as we do that wave of seeking in publicity that you guys will help and start to share and reach back into your networks and engage.

>> FRIEDMAN: So that is the plan going forward, which is we've got, working groups have their marching orders for finishing these documents. We're going to have them out by the first week of October and the second, first week-ish of October. You've got two weeks to get feedback on the draft documents. If you need a little light reading on the plane, make sure to grab your hard copy on the way out and we're going to try to tackle this very large set of things to do and I think that's a great place to sort of end things, which is to say we've made incredible progress. I don't want anyone to walk out of here without feeling really happy that this community, thanks to your hard work. This isn't NTIA, this is you, have actually said, Oh S bomb can really be a reality. This is something that is going to make us better off. We know what it is, we know why we should do it. We have an idea of how to do it, and we've seen that people actually did it, but that's not enough.

>> FRIEDMAN: We still have to do a lot more work on answering some of these remaining issues and having this broader outreach campaign as well. So with that, I think we can all relax after a day of pretty solid work. And if you're not running for a plane, there is a nearby place that we go to have a celebratory chat and to have some of these offline conversations where the work actually gets [inaudible]. So I hope, Oh yes, there's a question. And last, I want to thank Luis for helping us and for NTIA's brand new intern. So new that I'm going to butcher her name is Svancha?

>> SVANCHA: Yes.

>> FRIEDMAN: Svancha, who is a two L at Catholic Law so if anyone is looking for a technically literate lawyer, she'll be available in about a year and a half. So with that, thank you all. I thought that was a very productive meeting, and that concludes the webcast and the phone call. Thank you, Melinda.